现代数学基础丛书 104

椭圆与超椭圆曲线公钥密码的理论与实现

王学理　裴定一　著



科学出版社

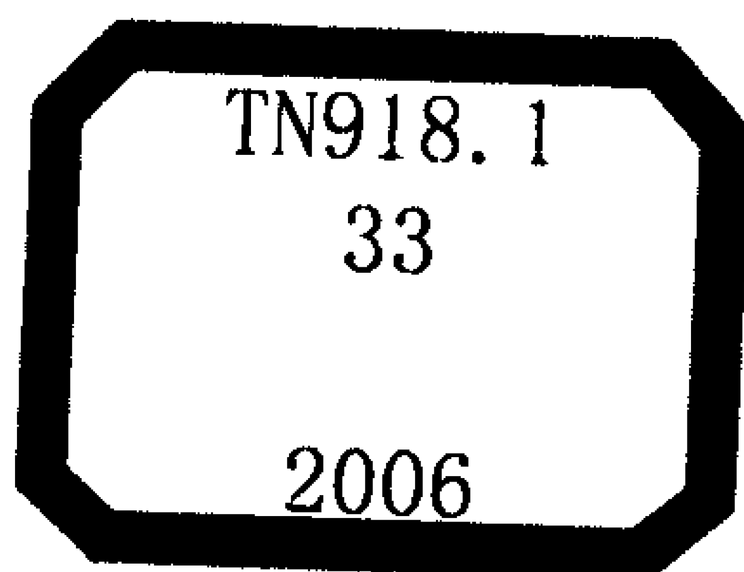
www.sciencep.com

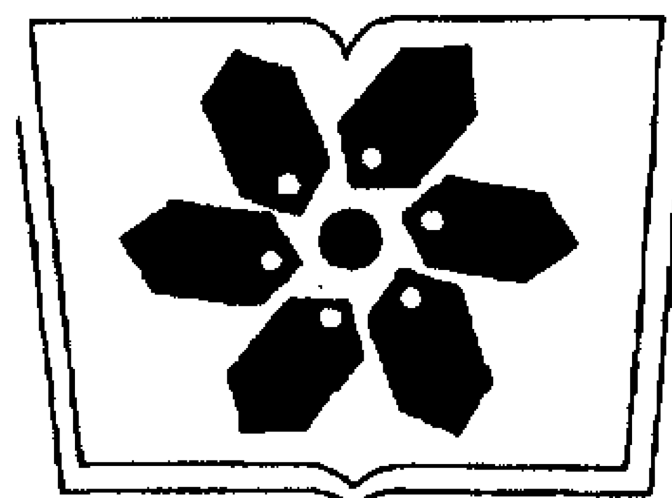
(O-2517.0101)



销售分类建议：高等数学

ISBN 7-03-017358-9
定 价：65.00 元





中国科学院科学出版基金资助出版

现代数学基础丛书　104

椭圆与超椭圆曲线公钥密码的理论与实现

王学理　裴定一　著

科 学 出 版 社
北　京

内 容 简 介

本书论述了椭圆与超椭圆曲线公钥密码学的基本理论及实现，其中包括：椭圆曲线公钥密码体制介绍，椭圆和超椭圆曲线的基本理论，定义在有限域上椭圆和超椭圆曲线的有理点的计数，椭圆和超椭圆曲线上的离散对数，椭圆和超椭圆曲线离散对数的初等攻击方法、指标攻击方法、代数几何攻击方法及代数数论攻击方法．本书的特点之一，内容涉及面广，在有限的篇幅内，包含了必要的预备知识和较完备的数学证明，尽可能形成一个完整的体系；特点之二，用较为系统和统一的方法总结了大部分有限域上椭圆和超椭圆曲线有理点的有效计数方法；特点之三，用系统的数学方法讲述了椭圆和超椭圆曲线离散对数攻击的主要有效方法；特点之四，我们总是从算法数论的角度进行论述，对每个重要的理论结果，总是尽可能给出其可编程的实际算法．本书的部分较初等的内容曾多次在中国科学院研究生院信息安全重点实验室及广州大学和湖南大学作为研究生教材使用．

本书可作为信息安全、数论及相关专业的研究人员、高等学校的教师和高年级学生的参考书，其部分内容也可做为信息安全、数论等专业的研究生的教材使用．

图书在版编目(CIP)数据

椭圆与超椭圆曲线公钥密码的理论与实现/王学理，裴定一 著．—北京：科学出版社，2006
(现代数学基础丛书；104)
ISBN 7-03-017358-9
I. 椭… II. ①王… ②裴… III. 椭圆曲线-密码-研究 IV. TN918.1
中国版本图书馆 CIP 数据核字(2006) 第 057318 号

责任编辑：陈玉琢／责任校对：包志虹
责任印制：安春生／封面设计：王 浩

科学出版社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
新蕾印刷厂 印刷
科学出版社发行 各地新华书店经销
*
2006 年 12 月第 一 版 开本：B5(720×1000)
2006 年 12 月第一次印刷 印张：30 3/4
印数：1—3 000 字数：586 000
定价：65.00 元
(如有印装质量问题，我社负责调换〈环伟〉)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言，书籍与期刊起着特殊重要的作用．许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍，从中汲取营养，获得教益．

20 世纪 70 年代后期，我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了十余年，而在这期间国际上数学研究却在迅猛地发展着．1978 年以后，我国青年学子重新获得了学习、钻研与深造的机会．当时他们的参考书籍大多还是 50 年代甚至更早期的著述．据此，科学出版社陆续推出了多套数学丛书，其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出，前者出版约 40 卷，后者则逾 80 卷．它们质量甚高，影响颇大，对我国数学研究、交流与人才培养发挥了显著效用．

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者，针对一些重要的数学领域与研究方向，作较系统的介绍．既注意该领域的基础知识，又反映其新发展，力求深入浅出，简明扼要，注重创新．

近年来，数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用，还形成了一些交叉学科．我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域．

这套丛书得到了许多数学家长期的大力支持，编辑人员也为其付出了艰辛的劳动．它获得了广大读者的喜爱．我们诚挚地希望大家更加关心与支持它的发展，使它越办越好，为我国数学研究与教育水平的进一步提高作出贡献．

杨　乐

2003 年 8 月

前　言

公钥密码是 20 世纪 70 年代中期提出的一类新型的密码, 它特别适合在计算机网络环境下使用, 具有信息加密、管理密钥和数字签名等功能, 能保证信息的机密性、完整性和不可否认性. 迄今为止, 所提出的公钥密码的安全性均建立于某个数学难题的基础之上, 这里所谓数学难题, 是指求解这个数学问题目前还没有多项式时间的算法被发现, 例如, 大整数的因子分解、有限域或椭圆曲线离散对数等问题, 在适当选取参数后, 在现有理论和技术条件下, 这些问题都难以解决, 这就奠定了相应的公钥密码的安全性基础, 而解决这些难题所取得的任何重大进展, 都会对相应的公钥密码的使用产生巨大的影响.

目前影响最大的三类公钥密码是 RSA 公钥密码、ElGamal 公钥密码和椭圆曲线公钥密码, 前者是在 20 世纪 70 年代中期提出的, 其安全性依赖于大整数的因子分解的困难性, 而后两者的安全性分别依赖于有限域和椭圆曲线离散对数的难度. 椭圆曲线公钥密码是 20 世纪 80 年代中期提出来的, 由于它具有一些其他公钥密码无法比拟的优势, 因此, 近年来对它的研究十分活跃, 而相关的研究所获得的许多算法, 大大丰富了算法数论和椭圆曲线密码的理论. 本书的主要目的就是介绍这方面的最新进展.

具有良好密码特性的椭圆曲线的产生和椭圆曲线离散对数的计算, 是椭圆曲线密码理论研究的两个核心问题, 而如何加快椭圆曲线的倍点运算, 则是椭圆曲线密码实现中的主要问题. 因此, 本书的主要内容就是介绍这三方面的基本理论, 及迄今为止所提出的主要算法的基本原理和实际算法实现. 主要内容分布如下：本书分五大部分, 第一部分是椭圆曲线密码体制介绍, 我们的叙述方式利用了可证明安全性的理论框架；第二部分是利用到整体域的提升方法计算有限域上椭圆曲线的有理点的数目, 主要包含复数域和一般域上椭圆曲线的一般理论以及复乘算法和 SEA 算法；第三部分是利用到局部域的提升方法计算有限域上椭圆曲线的有理点的数目, 主要包含局部域上椭圆曲线的基本理论、形式群以及 Satoh 算法、AGM 算法、Harley 算法、Kedlaya 算法等内容；第四部分介绍 (超) 椭圆曲线离散对数的攻击方法, 主要有基本的初等攻击方法、指标计算攻击方法、代数几何攻击和代数数论攻击方法；第五部分介绍椭圆曲线的倍点计算, 这是椭圆曲线密码实现中的主要问题.

下面我们简单介绍一下上面提到的有关内容. 在第一章中, 我们介绍了 IEEE P1363 标准中推荐的有关加密、签名等方案, 从这些方案的介绍中可以看出, 若要

实现它们, 则要找到具有良好密码特性的椭圆曲线, 并考虑椭圆曲线离散对数的安全性, 同时加快椭圆曲线的倍点运算. 我们在介绍了这些方案后, 就利用所谓可证明安全性的框架对这些方案进行讨论. 需要指出的是, 现在人们一般认为, 应该要求所给方案在某种安全性框架 (或曰模型) 下是可证明安全的, 至于在实际应用中需要什么框架下的可证明安全性, 则需要根据实际情况来决定. 在第二部分中, 我们介绍提升到整体域的椭圆曲线有理点点数计算方法, 其理论基础是 Deuring 的相关理论, 简单地说, 就是一条定义在有限域上的通常的椭圆曲线都可以提升到某条定义在某个代数数域上的椭圆曲线, 而它在模去某个理想后, 就回到了原来的有限域上定义的椭圆曲线, 这个提升的过程就使我们能将有限域上的问题转化为复数域上的相关问题. 而在复数域上, 就有很多的可供利用的工具, 如复乘理论、模形式理论等, 这就分别构成了复乘算法和 SEA 算法的基础, 这些算法对大特征和小特征的有限域都可以应用. 在第三部分中, 我们将刚才的 Deuring 的理论中的整体域换成局部域 (相应的 Deuring 理论依然成立), 就将有限域上的问题转化为局部域上的相应问题, 而利用局部域和有限域上椭圆曲线的关系 (Lubin-Serre-Tate 定理), 就可以得出 Satoh 算法. 而利用椭圆曲线的 2- 同种方法到相关的局部域上的椭圆曲线, 我们就得出 Mestre 的 AGM 算法. 如果我们应用 de Rham 上同调等工具到定义在局部域上的相关几何对象上 (椭圆或超椭圆曲线), 就得到 Kedlaya 算法. 在第四部分中, 我们介绍目前已知的各种对 (超) 椭圆曲线密码的攻击方法, 除了一些较初等的方法外, 我们主要介绍的方法有两类, 即代数几何的方法和代数数论的方法, 这两类方法的思想都来自 Gerhard Frey, 前者的主要工具是 Weil 下降, 而后者的主要工具是类域论 (特别是 Brauer 群理论), 前者的想法是利用 Weil 下降将椭圆曲线离散对数问题转化为另一类几何对象 (例如, 超椭圆曲线或高维 Abel 簇) 的离散对数问题, 而后者的想法是利用类域论的方法将椭圆曲线离散对数问题转化为 Brauer 群中的对应问题. 我们认为这两类方法均具有很好的研究前景, 而且由于此前还没有任何著述系统介绍这两类方法, 所以我们希望有兴趣的读者能深入了解这些理论. 最后, 我们在第五部分介绍了如何加快倍点运算的各种方法.

本书的选材经过精心考虑, 内容的涉及面很广, 在有限的篇幅内包含了必要的预备知识和数学证明, 从而形成了一个完整的体系. 我们写作本书的一个主要思想是: 既系统介绍有关的理论, 又详细给出这些理论的相关算法, 这样就能够真正使理论和应用很好地结合. 我们希望, 读者无论是只对算法实现感兴趣 (如相关的工程技术人员), 或只对理论感兴趣 (如数学研究工作者), 或对两者均感兴趣 (如公钥密码研究者), 都能从中有所裨益. 本书可作为数论和信息安全专业的研究人员和研究生的参考书. 如果作为研究生的教材, 则需要根据学生的情况对有关内容进行取舍. 本书的部分内容曾在中国科学院研究生院信息安全国家重点实验室和广州大学及湖南大学作为研究生教材使用.

在本书的编写过程中, 作者王学理曾多次应 Gerhard Frey 教授邀请访问 Essen 大学 IEM, 在此表示衷心的感谢. 在本书写作过程中, 董军武同志给予了作者十分重要的帮助, 并写作了第十九章的内容, 而高伟同志写作了第一章的部分内容, 在此一并感谢. 另外, 本书的编写得到国家自然科学基金 "低权模形式的构造及其在二次型和椭圆曲线中的应用"(批准号：10271042) 和国家 "973" 项目 "信息与网络安全体系结构"(批准号：G1999035804) 的资助, 特此感谢.

最后, 作者王学理特别要感谢他亲爱的妻子徐东平女士和他可爱的两个女儿毛毛、虫虫以及他的双亲和岳父母, 是他们的支持和爱使本书的完成成为可能.

作　者

2005 年 4 月 21 日

目　　录

第一部分　椭圆曲线密码体制

第二部分　提升到整体域上的点数计算算法

第三部分　提升到局部域上的点数计算算法

第四部分　椭圆曲线密码体制的攻击方法

第五部分 椭圆曲线密码体制的实现

* * *

第一部分

椭圆曲线密码体制

第一章　椭圆曲线密码体制

在本章中, 首先引进有限域上的椭圆曲线及其上的加法运算, 然后给出椭圆曲线公钥密码体制的加密、解密、签名等方案.

§1.1　有限域上的椭圆曲线

设 p 为一素数, n 为正整数, $q=p^n$, 而 $\mathbb{F}_q$ 是 q 个元素的有限域, 记 $\mathbb{F}_q$ 的代数闭包为 $\overline{\mathbb{F}}_q$. $\mathbb{F}_q$ 上的 Weierstrass 方程式

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\quad a_i\in\mathbb{F}_q. \tag{1.1}$$

决定仿射平面 $\mathbb{A}^2(\overline{\mathbb{F}}_q)$ 上一条曲线, 添加上无穷远点后, 就得到射影平面 $\mathbb{P}^2(\overline{\mathbb{F}}_q)$ 上的一条曲线 E, 若曲线 E 是非奇异的, 则 E 称为一条椭圆曲线. 可以证明 E 是一条椭圆曲线, 当且仅当判别式 $\Delta\neq 0$, 其中

$$\begin{aligned}
&\Delta=-b_2^2b_8-8b_4^3-27b_8^2+9b_2b_4b_6,\\
&b_2=a_1^2+4a_2,\\
&b_4=2a_4+a_1a_3,\\
&b_6=a_3^2+4a_6,\\
&b_8=a_1^2a_6+4a_2a_6-a_1a_3a_4+a_2a_3^2-a_4^2.
\end{aligned} \tag{1.2}$$

有关证明参见 §3.1. 我们定义 E 的 j 不变量如下:

$$j=c_4^3/\Delta,\quad c_4=b_2^2-24b_4. \tag{1.3}$$

给定一条 $\mathbb{F}_q$ 上的椭圆曲线 E, 及其上任意两点 P 和 Q, 连接 P 和 Q 的直线与 E 交于第 3 个点 R, 由 R 和无穷远点 O 可决定一直线, 该直线与 E 的第 3 个交点定义为 P 与 Q 的和, 记为 $P\oplus Q$. 可以证明这样定义 E 上点的加法后, 就使 E 成为一个 Abel 群. 由上面的加法的定义, 可给出具体的加法公式如下:

设 E 是由 (1.1) 式定义的椭圆曲线, 我们有

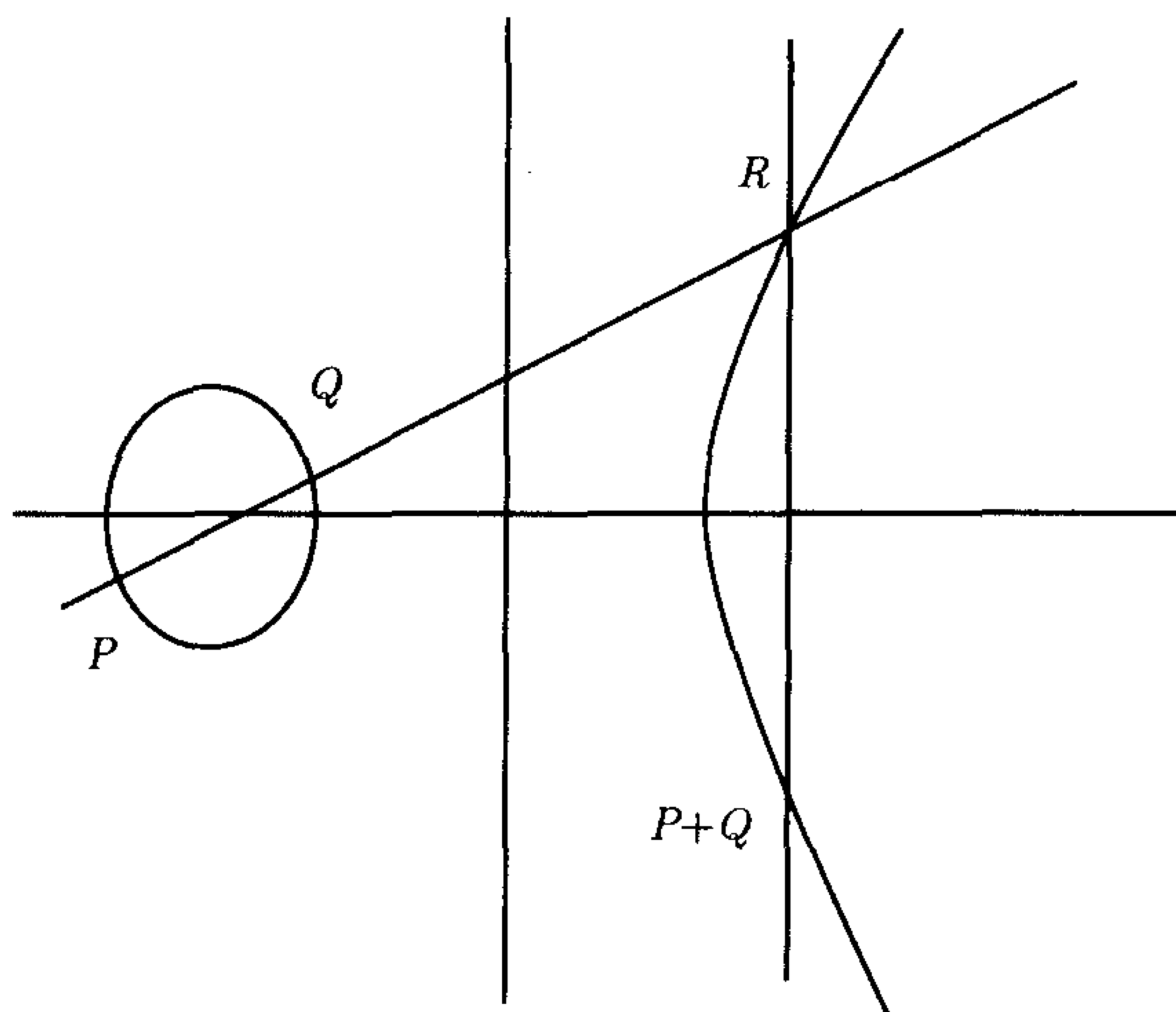
(a) 设 $P=(x,y)\in E$, 则 $-P=(x,-y-a_1x-a_3)$, 设

$$P_1+P_2=P_3,\quad P_i=(x_i,y_i)\in E,\quad i=1,2,3.$$

(b) 若 $x_1 = x_2$, $y_1 + y_2 + a_1x_1 + a_3 = 0$, 则 $P_1 + P_2 = \mathcal{O}$, 否则, 令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{当 } x_1 \neq x_2 \text{ 时}, \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{当 } x_1 = x_2 \text{ 时}, \end{cases}$$

$v = y_1 - \lambda x_1$.



(c) P_3 由下式给出：

$$x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2,$$
$$y_3 = \lambda(x_1 - x_3) - y_1 - a_1x_3 - a_3.$$

特别地, 当 $P_1 \neq P_2$ 时,

$$x(P_1 + P_2) = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 + a_1\left(\frac{y_2 - y_1}{x_2 - x_1}\right) - a_x - x_1 - x_2,$$

当 $P_1 = P_2$ 时,

$$x(2P_1) = \frac{x_1^4 - b_4x_1^2 - 2b_6x_1 + b_8}{4x_1^3 + b_2x_1^2 + b_4x_1 + b_6},$$

其中 b_i 如 (1.2) 式定义.

另外, 可以证明, 当 $p \neq 2, 3$ 时, 每一条 $\mathbb{F}_q$ 上的椭圆曲线都同构于下述形式的一条椭圆曲线：

$$E: \quad y^2 = x^3 + ax + b, \quad a, b \in \mathbb{F}_q.$$

当 $p=3$ 时, $\mathbb{F}_q$ 上每一条椭圆曲线均同构于

$$E:\quad y^2=x^3+a_4x+a_6,\quad 若\ j=0,$$

或

$$E:\quad y^2=x^3+a_2x^2+a_6,\quad 若\ j\neq 0.$$

当 $p=2$ 时, $\mathbb{F}_q$ 上每一条椭圆曲线均同构于

$$E:\quad y^2+a_3y=x^3+a_4x+a_6,\quad 若\ j=0,$$

或

$$E:\quad y^2+xy=x^3+a_2x^2+a_6,\quad 若\ j\neq 0.$$

现在令

$$E(\mathbb{F}_q)=\{(x,y)\in E|x\in\mathbb{F}_q,y\in\mathbb{F}_q\}\bigcup\{\mathcal{O}\}.$$

不难看出, $E(\mathbb{F}_q)$ 是 $E(\overline{\mathbb{F}}_q)$ 的一个子群. 可以证明

$$|\#E(\mathbb{F}_q)-q-1|\leqslant 2\sqrt{q}$$

(参见 §3.5).

一般来说, 我们总是选取有限域 $\mathbb{F}_q$ 为下述二者之一: 或者 $\mathbb{F}_q$ 是一个素域 $\mathbb{F}_p$, 或者 $\mathbb{F}_q$ 是 $\mathbb{F}_{2^m}$(m 为某个素数), 我们这样选取是为了安全性的考虑 (参见本书第四部分).

§1.2 椭圆曲线公钥密码体制

一、体制建立

首先建立椭圆曲线密码体制: 选取一个基域 $\mathbb{F}_q$, 它或者是一个素域 $\mathbb{F}_p$, 或者是一个特征 2 的域 $\mathbb{F}_{2^m}$, 其中 m 为素数. 然后选取 $\mathbb{F}_q$ 上的一条椭圆曲线 E, 使其阶为一个大素数 n, 或者是一个大素数 n 与另一个小整数的乘积. 而后, 选取 E 上的一个阶为该大素数 n 的点 P. 于是, 有限域 $\mathbb{F}_q$、曲线 E、点 P 和其阶 n 均为公开的信息.

二、密钥生成

每一个参与者 (或者说用户)A 完成下述过程:

1. 随机选取一个整数 $d_A\in[1,n-1]$;
2. 计算点 $Q_A=d_AP$;
3. 该参与者的公钥为点 Q_A;
4. 该参与者的私钥为整数 d_A.

三、椭圆曲线加密方案 (ECES)

现在设用户 B 要发送信息 M 给用户 A, 则 B 的加密过程如下：

1. 找出 A 的公钥 Q_A;
2. 将信息 M 表示为一个域元素 $m \in \mathbb{F}_q$;
3. 随机选取一个整数 $k \in [1, n-1]$;
4. 计算点 $(x_1, y_1) = kP$;
5. 计算点 $(x_2, y_2) = kQ_A$, 若 $x_2 = 0$, 则返回第 3 步;
6. 计算 $c = m \cdot x_2$;
7. 将已加密数据 (x_1, y_1, c) 发送给 A.

而 A 收到密文 (x_1, y_1, c) 后的解密过程如下：

1. 计算点 $(x_2, y_2) = d_A(x_1, y_1)$, 得出 $x_2 \in \mathbb{F}_q$;
2. 计算 $m = c \cdot x_2^{-1}$, 得出信息 M.

下面我们讨论该方案的安全性与问题难解性假设之间的关系. 我们不打算从严格形式化的角度来讨论密码系统的安全性, 而是更多地专注于密码学的数学理论. 如对严格定义和形式化证明感兴趣 (如概率多项式时间算法、不可忽略性、显著、CCA,CPA 等), 可参看文献 [1].

定义 1.1 (全有或全无安全性 (all-or-nothing))　*在此模型下, 对给定的加密算法及一个给定密文, 攻击者的目的是计算与之对应的整个明文; 或者根据加密算法及给定的一个明密文对, 攻击者试图计算出该算法对应的整个解密密钥. 攻击者要么成功即能够获得整个明文分组或者解密密钥, 要么失败即没有获得任何信息. 这里所谓“没有任何信息”是指攻击者无论攻击前后都没有掌握所要攻击的目标 (整个明文或解密密钥) 的任何信息.*

定义 1.2 (被动攻击)　*在该模型下, 攻击者不能操纵和修改它所掌握的密文, 并且不能从加密方获得 (对非攻击目标的) 加密或解密服务.*

定义 1.3 (选择明文攻击 (CPA))　*在这种攻击模型下, 攻击者可以选择任何明文并且获得其相应的密文, 并在此基础上试图降低密码系统的安全性 (如对于攻击的目标密文, 获得明文的若干比特, 或者获得整个明文).*

易知, 对于任何的公钥密码系统, 攻击者可以根据加密算法和加密公钥发起选择明文攻击.

定义 1.4 (椭圆曲线计算性 Diffie-Hellman 问题 (ECCDH))

Input：*基域 $\mathbb{F}_q$ 及其上的椭圆曲线 E, E 上的阶为素数 n 的点 P, aP, bP, 这里 $a, b \in_R \mathbb{Z}_n^*$ (这里符号 $\in_R$ 表示随机均匀选取, 以下同).*

Output：*abP.*

而所谓 ECCDH 假设即假设不存在有效的算法 (概率多项式时间的算法, 其成功概率不可忽略, 以下同) 解决该问题.

定理 1.1 对于以均匀概率取自整个明文空间的明文, ECES 在选择明文攻击下是“全有或全无”安全 (all-or-nothing secure) 的当且仅当 ECCDH 问题是困难的.

证明 ($\Rightarrow$) 反证法. 假设存在概率多项式时间的算法以不可忽略的概率解决 ECCDH 问题. 对于 ECES 下的一个密文 $(x_1, y_1, c) = (kP, m \cdot x_2)$(参数同 ECES, 以下同), 由假设知道根据随机信息 kP 和公钥 $Q = dP$ 可有效地计算出 $kdP = kQ = (x_2, y_2)$, 因此可计算明文 $m = c \cdot x_2^{-1}$, 从而 ECES 不是全有或全无安全的, 出现矛盾, 假设不成立.

($\Leftarrow$) 反证法. 假设存在有效的算法 $\mathcal{O}$ 攻击 ECES, 也就是说给定公钥 Q 及公共参数 $(E(\mathbb{F}_q), P, n)$ 和密文 $(x_1, y_1, c) = (kP, c)$,$\mathcal{O}$ 可以有效地计算出相应明文 $m = \mathcal{O}(Q, E(\mathbb{F}_q), P, n, x_1, y_1, c) = c \cdot x_2^{-1}$. 对于 ECCDH 问题, 根据其输入 aP, bP 构造 ECES 的公钥为 $Q = aP$, 随机信息 $kP = bP = (x_1, y_1)$, 选取 $c \in_R \mathbb{F}_q$, 从而构造出密文 $(x_1, y_1, c) = (bP, c)$, 把这些信息及公共参数作为输入调用 $\mathcal{O}$, 则以不可忽略的概率可获取其输出 (bP, c) 对应的明文 m, 从而可以计算 abP 的横坐标 $x_2 = c \cdot m^{-1}$, 进而可以算出 abP(这里 m 在 $\mathbb{F}_q$ 中不可逆的概率可忽略), 这与 ECCDH 假设矛盾, 证毕.

定义 1.5 (密文的不可区分性 (indistinguishability)) 所谓密文的不可区分性, 是指不存在多项式时间的攻击者能够以“显著”超过 1/2 的概率区分两个已知的不同明文对应的密文, 或者分辨出给定明文的密文和随机字符串, 在选择明文攻击下达到这种要求的密码系统又称为语义安全的. (为了避免过于形式化, 这里用了“不可忽略”、“显著”等易于理解但并不非常准确的描述; “或者”前后的两个分句条件是等价的. 如需深刻描述可参阅文献 [1], 以下同.)

定义 1.6 (椭圆曲线判定性 Diffie-Hellman 问题 (ECDDH))

Input: 基域 $\mathbb{F}_q$ 及其上的椭圆曲线 E, E 上的阶为素数 n 的点 P, aP, bP, cP, 这里 $a, b, c \in_R \mathbb{Z}_n^*$.

Output: 如果 $cP = abP$, 输出 1, 否则输出 0.

而所谓 ECDDH 假设即假设不存在有效的算法 (概率多项式时间的算法, 其成功概率显著超过 1/2) 解决该问题.

定理 1.2 ECES 在选择明文攻击下是语义安全的等价于 ECDDH 问题是困难的.

证明 ($\Rightarrow$) 反证法. 假设存在有效算法 $\mathcal{O}$ 解决 ECDDH 问题, 则可以通过如下构造来攻击 ECES. 对于给定明文对 (m_1, m_2), 密文 $c_b = (kP, c') = (x_1, y_1, c')$, 及 EDES 所指定的公钥 $Q = dP$ 和系统参数 (E, P, n), 计算 $x_2 = c' \cdot m_1^{-1}$, 进而计算

点 (x_2, y_2), 然后以 $aP = Q = dP, bP = kP = (x_1, y_1), cP = (x_2, y_2)$ 及其 ECES 的公共参数为输入调用 $\mathcal{O}$, 若输出 1, 则认为 c_b 为 m_1 的密文, 否则为 m_2 的密文. 这里, 我们易知, 如果 c_b 恰好是 m_1 的密文, 则必有 $(x_2, y_2) = dkP = abP$, 从而 $\mathcal{O}$ 以显著超过 1/2 的概率输出 1, 此时我们的判断 c_b 是 m_1 的密文也是以显著 1/2 的概率是正确的; 反之, 如果 c_b 是 m_2 的密文, 则必有 $x_2' = c' * m_2^{-1}$, 进而计算点 $(x_2', y_2') = abP = dkP \neq (x_2, y_2) = cP$, 此时 $\mathcal{O}$ 能够以显著超过 1/2 的概率输出正确的判断 0, 从而此时的判断 c_b 为 m_2 的密文也是以显著的概率是正确的. 这样, 我们上面描述的算法可以显著超过 1/2 的概率攻破 ECES 的语义安全性.

($\Leftarrow$) 反证法. 假设 ECES 在选择明文攻击下不是语义安全的, 即存在概率多项式时间的算法 $\mathcal{O}$ 在给定公钥 Q、系统参数 (E, n, P)、明文 m_1 和密文 $c_b = (kP, c') = (x_1, y_1, c')$ 时可以判断 c_b 是 m_1 对应的密文, 还是一个随机数, 且其成功概率显著地高于 1/2. 我们用如下构造来解决 ECDDH 问题. 给定 aP, bP, cP 及其系统参数 (E, n, P), 选取一个明文 $m_1 \in \mathbb{F}_q$, 取公钥为 $dP = aP$, 随机信息 $Q = bP$, 设 $cP = (x_2, y_2)$, 并计算 $c_0 = m_1 \cdot x_2$, 从而构造的密文为 $c_b = (bP, c_0)$. 如果 $abP = cP$, 则 c_b 为 m_1 的合法密文, 否则由 cP 的随机性, 可知 c_b 也是随机的. 而 $\mathcal{O}$ 可以显著超过 1/2 的概率区分这两种情形, 从而我们可以显著超过 1/2 的正确概率判断是否 $abP = cP$, 证毕.

定义 1.7 (选择密文攻击) *该攻击模型是指攻击者可以获得除所攻击的密文以外的任何密文的明文.*

定理 1.3 ECES *在选择密文攻击下是全有或全无意义下不安全的.*

证明 给定公钥 Q、公共参数 (E, n, P) 和所要攻击的密文 (x_1, y_1, c), 构造新的密文 (x_1, y_1, c'), 这里 $c' \in_R \mathbb{F}_q$, 由于攻击模型为选择密文攻击, 攻击者可以获得任何不等于目标密文的密文所对应的明文, 从而攻击者可以获得 $(x_1, y_1, c') \neq (x_1, y_1, c)$ 的明文 m', 计算 $x_2 = c' \cdot m'^{-1}$, 进而可计算所要攻击的明文 $m = c \cdot x_2^{-1}$, 证毕.

四、椭圆曲线签名方案 (ECSS 和 ECDSA)

我们给出两个签名方案, 一个称之为 ECSS, 另一个称为 ECDSA.

ECSS 签名生成: 设用户 A 要对信息 M 签名后, 给用户 B, 则 A 要完成下述步骤:

1. 将 M 表为比特串;
2. 应用 Hash 算法 H 计算出 Hash 值 $e = H(M)$;
3. 随机选取整数 $k \in [1, n-1]$;
4. 计算点 $(x_1, y_1) = kP$;
5. 计算 $r = x_1 + e$;
6. A 应用自己的私钥 d_A 计算 $s = k - d_A r \pmod n$;

7. A 将信息 M 和签名 (r,s) 发送给 B.

ECSS 签名验证：设 B 收到 A 对信息 M 的签名 (r,s), 需要验证是否为 A 所签, 则 B 要完成下述过程：

1. 找出 A 的公钥 Q_A;
2. 计算点 $(x_1,y_1)=sP+rQ$;
3. 计算 Hash 值 $e=H(M)$;
4. 计算 $r'=x_1+e$;
5. 当且仅当 $r=r'$ 时, A 对信息 M 的签名被 B 认可.

ECDSA 签名生成：设用户 A 要对信息 M 签名后给用户 B, 则 A 要完成下述步骤：

1. 将 M 表为比特串;
2. 应用 Hash 算法 H 计算出 Hash 值 $e=H(M)$;
3. 随机选取整数 $k\in[1,n-1]$;
4. 计算点 $(x_1,y_1)=kP$, 令 $r=x_1 \pmod n$, 若 $r=0$, 返回第 3 步;
5. A 应用自己的私钥 d_A 计算 $s=k^{-1}(e+rd_A) \pmod n$, 若 $s=0$, 则返回第 3 步;
6. A 将信息 M 和签名 (r,s) 发送给 B.

ECDSA 签名验证：设 B 收到 A 对信息 M 的签名 (r,s), 需要验证是否为 A 所签, 则 B 要完成下述过程：

1. 找出 A 的公钥 Q_A;
2. 计算 Hash 值 $e=H(M)$;
3. 计算 $s^{-1} \bmod n$;
4. 计算 $u=s^{-1}e \bmod n$ 和 $v=s^{-1}r \bmod n$;
5. 计算点 $(x_1,y_1)=uP_1+vQ_A$;
6. 当且仅当 $x_1 \bmod n=r$ 时, A 对信息 M 的签名被 B 认可.

定义 1.8 (适应性选择消息攻击) 设 k 是一个正整数, 称作安全参数. 对于签名方案 (gen, sign, verify) 一个适应性伪造者是一个概率多项式时间 (对于参数 k) 的算法. 它以 pk 为输入 (这里 (pk,sk) 是由 $\text{Gen}(1^k)$ 随机产生的密钥对), 力图伪造公钥 pk 下的签名, 而伪造者可以获得它所选择的任何消息的签名 (当然非试图伪造的签名). 这种攻击称作适应性选择消息攻击. 如果不存在概率多项式时间的伪造者可以不可忽略的概率伪造一个有效的签名, 则称该签名方案是在选择消息攻击下是可以抵抗存在性伪造的.

基于离散对数难解性的数字签名 (ElGamal-like-signature) 实际上是对消息的 hash 值做相应的签名, 一方面只要正确使用这些方案, 在离散对数的困难性和 Hash 函数的安全性的合理假设下, 似乎在选择消息攻击下是可以抵抗存在性伪造的; 另

一方面只有一类比较特殊的变形 (triplet ElGamal-family signature [1]) 在 Random Oracle 模型 (将 Hash 函数假设为可访问的随机函数) 和离散对数困难假设下可以证明在选择消息攻击下是可以抵抗存在性伪造的, 不过其他签名稍加改造即可变为这种类型. 例如 DSA 及其变形 ECDSA, 作为标准, 在经过了广泛的研究下, 人们并没有发现有效攻击方案, 但是也没有给出其安全性证明 (即将其安全性等价于离散对数问题难解性假设). 正如 NealKoblitz 所说, DSA 稍微改变一下就可以加上可证明安全性, 但是在诸多个人和公司对该标准的反对声中却忘记了这个可能是最合理的理由.

五、椭圆曲线密钥生成协议 (ECKEP)

我们现在给出一个产生会话密钥的协议. 首先假定两个用户 A 和 B 应用相同的椭圆曲线参数: $\mathbb{F}_q$, E, P 和 n. A 的私钥为 d_A, B 的私钥为 d_B. 而 A 和 B 的公钥分别为 $Q_A = d_AP = (x_A, y_A)$ 和 $Q_B = d_BP = (x_B, y_B)$.

1. A 完成下述步骤:

(a) 随机选取整数 $k_A \in [1, n-1]$;

(b) 计算点 $(x_1, y_1) = R_A = k_AP$;

(c) A 将 R_A 发送给 B.

2. B 完成下述步骤:

(a) 随机选取整数 $k_B \in [1, n-1]$;

(b) 计算点 $(x_2, y_2) = R_B = k_BP$;

(c) B 将 R_B 发送给 A.

3. A 完成下述步骤:

(a) 计算整数 $S_A = k_A + x_1d_Ax_A \pmod n$;

(b) 计算会话密钥 $K = S_A(R_B + x_2x_BQ_B)$.

4. B 完成下述步骤:

(a) 计算整数 $S_B = k_B + x_1d_Bx_B \pmod n$;

(b) 计算会话密钥 $K = S_A(R_A + x_2x_AQ_A)$.

定义 1.9 (内在认证性 (implicit authentication)) *所谓内在认证性是指协商密钥的一方可以断定除对方以外的任何方都不能破解所协商的密钥.*

定理 1.4 *在 ECCDH 问题难解的假设下, 上述方案可证明具有内在认证性.*

证明 在上述协议中, 所协商的密钥为 $k_Ak_BP + x_2x_Bk_Ad_BP + x_1x_Ad_Ak_BP + x_1x_Ax_2x_Bd_Ad_BP$, 故任何的被动攻击者根据 Q_A, Q_B, R_A, R_B 要想获得该协商密钥必定要计算 $d_Ad_BP, d_Ak_BP, d_Bk_AP, k_Ak_BP$, 而根据 ECCDH 问题的难解性知这是不可能的, 从而, 该方案具有内在认证性, 证毕.

上述方案并不提供密钥的确认性 (key confirmation), 即协商密钥的一方并不能判定它所获得的协商密钥是否为双方所试图协商的密钥, 因为 R_A 和 R_B 由于缺乏认证性而可能被主动攻击者所替换, 这也是存在对于上述方案的中间攻击的原因所在.

另外, 该方案是非交互的, 即通信双方的信息是相互无关的; 是角色对称的 (交换信息具有相同结构); 是前向安全 (forward secrety) 的, 即某一次的协商密钥的泄露并不会导致之前通信的安全性, 因为每次产生的协商密钥都与该次的随机信息 R_A 和 R_B 相关, 故各次通信所协商的密钥互不相关.

§1.3 基于双线性对的密码方案

Joux 在 2000 年发现利用椭圆曲线及其上的 Weil 对可以方便地构造三方密钥协商协议. 随后几年, 人们围绕椭圆曲线及其上的 Weil 对或 Tate 对构造了各种各样的公钥密码系统, 如基于身份的签名、加密、签密、短签名、密钥协商协议、分等级加密和签名等, 充分显示了椭圆曲线理论在应用密码学中的威力[2].

定义 1.10 (具有密码学意义的双线形对 (以下简称对)) *设 G_1 和 G_2 是两个阶同为素数 q 的群, 其中 G_1 为加法群, G_2 为乘法群, P 是 G_1 的生成元. 假设 G_1 和 G_2 中的离散对数是难解的. 一个具有密码学意义的双线形对是指具有如下性质的映射 $e: G_1^2 \to G_2$:*

双线性: 对任给的 $P, Q \in G_1, a, b \in \mathbb{Z}_q^*$, 都有 $e(aP, bQ) = e(P, Q)^{ab}$.

非退化性: 对于生成元 P 有: $e(P, P) \neq 1$.

可计算性: 对任意的 $P, Q \in G_1$, 存在有效的算法计算 $e(P, Q)$.

椭圆曲线上的 Tate 对和 Weil 对是目前构造具有密码意义双线性对所一致采用的途径[3]. 下面给出一个具体的构造:

设 $p > 3$ 是一个大素数, 它满足: $p \equiv 2 \pmod 3$, $q | p+1$ 是一个大素数. E 是一条定义在 $\mathbb{F}_p$ 上的椭圆曲线, 其方程为: $y^2 = x^3 + 1$. 对此, 易知如下事实:

事实 1 $E(\mathbb{F}_p)$ 包含 $p+1$ 个点, 其中无穷远点为 $\mathcal{O}$, 设 P 是 $E(\mathbb{F}_p)$ 中阶为 q 的点, $G_1 = \langle P \rangle$.

事实 2 对于任意的 $y_0 \in \mathbb{F}_p$, 存在惟一的点 $(x_0, y_0) \in E(\mathbb{F}_p)$, 这里 $x_0 = (y_0^2 - 1)^{1/3} \in \mathbb{F}_p$. 所以如果 (x, y) 是 $E(\mathbb{F}_p)$ 中随机点, 则 y 是 $\mathbb{F}_p$ 中的随机点.

事实 3 设 $1 \neq \zeta \in \mathbb{F}_{p^2}$ 是 $x^3 - 1 \equiv 0 \pmod p$ 的解, 则映射 $\phi(x, y) = (\zeta x, y)$ 是椭圆曲线 E 上的点群的同构. 对于 $Q = (x, y) \in E(\mathbb{F}_p)$, 总有 $\phi(Q) \in E(\mathbb{F}_{p^2})$. 所以, $Q \in E(\mathbb{F}_p)$ 与 $\phi(Q) \in E(\mathbb{F}_{p^2})$ 线性无关.

事实 4 因为 $P \in E(\mathbb{F}_p)$ 与 $\phi(P)$ 线性无关, 它们生成的群同构于 $\mathbb{Z} \times \mathbb{Z}$, 记作 $E[q]$.

设 G_2 是 $\mathbb{F}_{p^2}^*$ 的 q 阶子群. Weil 对 $\hat{e}$ 是从 $E[q]\times E[q]$ 到 G_2 的映射, 且是退化的, 即对于任意的 $P,Q\in E(\mathbb{F}_p)$, 都有 $\hat{e}(P,Q)=1$. 而如下的所谓修改的 Weil 对则是非退化的：

$$e(P,Q)=\hat{e}(P,\phi(Q)),$$

从而根据 Weil 对的定义 (可参考后续章节) 易验证修改的 Weil 对 $e:G_1^2\to G_2$ 是具有密码学意义的双线性对. 而椭圆曲线上的 Tate 对也可以构造双线性对, 我们不做具体介绍.

下面给出基于双线性对密码学的几个问题及其假设, 它们都是以椭圆曲线与有限域乘法群上的离散对数难解为最根本的假设.

1. (G_1,G_2,e) 中的**双线性的计算性 Diffie-Hellman 问题 (BDH)**

Input：(aP,bP,cP), 这里 $a,b,c\in_R\mathbb{Z}_q^*$,

Output：$e(P,P)^{abc}$.

2. (G_1,G_2,e) 中的**双线性的判定性 Diffie-Hellman 问题 (BDDH)**

Input：(aP,bP,cP,r), 这里 $a,b,c\in_R\mathbb{Z}_q^*, r\in G_2$,

Output：如果 $e(P,P)^{abc}=r$, 输出 1, 否则输出 0.

我们来简单分析一下这两个困难问题. 如果存在有效算法 $\mathcal{O}(,)$ 可以处理 G_1 中的计算性 Diffie-Hellman 问题, 即椭圆曲线的 ECCDH 问题, 那么可以通过如下算式处理 BCDH 问题：

$$e(P,P)^{abc}=e(\mathcal{O}(aP,bP),cP)=e(abP,cP);$$

如果存在有效 $\mathcal{O}'(,)$ 可以处理 G_2, 即有限域乘法群上的离散对数, 则

$$e(P,P)^{abc}=\mathcal{O}'(e(aP,bP),e(cP,P))=\mathcal{O}'(e(P,P)^{ab},e(P,P)^{c})=e(P,P)^{abc}.$$

由此可见, 椭圆曲线离散对数问题难解是具有密码学意义的双线性对的必要条件. 下面, 我们简单介绍几种常见的基于双线性对的密码方案. 在以下叙述中, 公开参数 G_1,G_2,q,e,P 如定义 1.10 中所给.

一、Joux 的一轮三方密钥协商协议

2000 年, Joux[4] 第一次将椭圆曲线上的 Weil 对和 Tate 对用于密码方案的构造, 而以往这两个工具则是用到密码分析中：将椭圆曲线上的离散对数问题化为有限域乘法群上的离散对数问题. Joux 利用双线性对构造的协议只要一轮通信过程即可使三方协商一个密钥, 而传统密钥协商协议至少需要两轮通信才能达到同样的目的, 其安全性则由 CBDH 问题的难解性所保证. 这一工作引发了人们对基于双线性对的密码学的研究热情, 随后涌现了大量的基于双线性对的密码方案, 同时也刺激了人们对超奇异的椭圆曲线的深入研究. 下面给出该协议的具体内容：

协议如下：考虑三方 A,B,C, 各自拥有私钥 $a, b, c \in \mathbb{Z}_q^*$:

A 发送 aP 给 B,C,

B 发送 aP 给 A,C,

C 发送 aP 给 A,B,

A 计算 $K_A = e(bP, cP)^a$,

B 计算 $K_B = e(aP, cP)^b$,

C 计算 $K_C = e(aP, bP)^c$,

协商的密钥为：$K_{ABC} = K_A = K_B = K_c = e(P, P)^{abc}$.

易知, 上述协议是 Diffie-Hellman 密钥协商协议的自然推广, 在 BCDH 假设下可以抵抗被动攻击. 当然该方案并不具备确认性 (key confirmation), 从而不能抵抗中间攻击, 但是基于该方案的一些变形则可以避免这样攻击, 如在方案的基础上辅以基于身份的签名[5].

二、基于身份的加密方案

协议如下[6]:

系统建立: 选择 $s \in_R \mathbb{Z}_q^*$, 计算 $P_{pub} = sP$. 选择两个 Hash 函数 $H_1 : \{0,1\}^* \rightarrow G_1^*$ (H_1 比较特殊, 称作 MapToPoint[6] 以下同) 和 $H_2 : G_2 \rightarrow \{0,1\}^n$, 其中 n 表示明文分组的长度. s 做主密钥, P_{pub} 做系统公钥.

授权个人私钥: 给定某用户的身份信息 $ID \in \{0,1\}^*$, 计算公钥 $Q_{ID} = H_1(ID) \in G_1$ 和用户私钥 $S_{ID} = sQ_{ID}$.

加密: 选择随机信息 $r \in \mathbb{Z}_q^*$, 计算明文 M 对应的密文为: $C = \langle rP, M \oplus H_2(e(Q_{ID}, P_{pub})^r)\rangle$.

解密: 给定密文 $C = \langle U, V\rangle$, 计算明文 $V \oplus H_2(e(S_{ID}, U))$.

上述方案类似于一般的 Elgamal 加密方案, 在 BCDH 问题难解的假设和 Random Oracle 模型下可证明是语义安全的 (抵抗 IND-ID-CPA[6]). 而达到这种安全性的加密方案通过所谓的 Fujisaki-Okamoto 转换即可获得在选择密文攻击下的密文不可区分安全性 (IND-ID-CCA[6]). 这是第一个实用有效的基于身份的加密方案.

三、短签名方案

协议如下[7]:

密钥产生: 设 $H : \{0,1\}^* \rightarrow G_1$(MapToPoint) 为 Hash 函数. 私钥为 $s \in_R \mathbb{Z}_q^*$, 公钥为 $P_{pub} = sP$.

签名: 给定消息 $m \in \{0,1\}^*$ 和私钥 s, 计算签名 $\sigma = xH(m)$.

验证: 给定公钥 $P_{pub} = xP$, 消息 m 和 σ, 验证是否 $e(P, \sigma) = e(P_{pub}, H(m))$.

该签名方案具有在 Random Oracle 模型下可证明的安全性：只要 G_1 中的 CDH 问题难解则该方案抵抗选择消息攻击下的存在性伪造. 一方面该方案的签名只有 160 比特, 另一方面其安全性与 320 比特的 DSA 签名相当, 是最短的安全签名方案.

四、基于身份的签名

其协议如下[8]：

系统建立：选择 $s \in_R \mathbb{Z}_q^*$ 作为主密钥, 计算 $P_{pub} = sP$ 做系统公钥. $H_1 : \{0,1\}^* \times G_1 \to \mathbb{Z}_q$ 和 $H_2 : \{0,1\}^* \to G_1$ 是两个 Hash 函数.

私钥产生：同基于身份的加密方案.

签名：给定签名私钥 $S_{ID} = sQ_{ID}$ 和消息 m, 选择 $r \in_R \mathbb{Z}_q$, 计算 $U = rQ_{ID}$, $h = H_1(m, U)$, $V = (r+h)S_{ID}$, 则签名为 $\sigma = (U, V)$.

验证：给定消息 m, 公钥 Q_{ID} 和签名 (U, V) , 计算 $h = (m, U)$, 验证 $e(P, V) = e(P_{pub}, U + hQ_{ID})$ 是否成立.

根据 CDH 问题的难解性, 这种基于身份的签名具有在 Random Oracle 模型下可证明安全性：可抵抗选择消息, 选择身份的存在性伪造.

五、基于身份的签密方案

其协议如下[9]：

系统建立：选择 $s \in_R \mathbb{Z}_q^*$ 为系统私钥, 计算 $P_{pub} = sP$ 为系统公钥. 选择一种对称加密算法 (E, D), 其私钥空间为 K_s, 密文空间为 C_s. $H_1 : \{0,1\}^* \to G_1(\text{MapToPoint})$, $H_2 : G_2 \to K_s$, $H_3 : C_s \times G_2 \to \mathbb{Z}_q$ 为 Hash 函数.

私钥产生：同基于身份的加密方案.

签密：给定消息 $m \in \{0,1\}^l, S_{ID_a}, ID_b$, 计算 $Q_{ID_b} = H_1(ID_b)$. 选择 $x \in_R \mathbb{Z}_q^*$, 计算 $k_1 = e(P, P_{pub})^x$, $k_2 = H_2(e(P_{pub}, Q_{ID_b})^x)$. 计算 $c = E_{k_2}(m), r = H_3(c, k_1), S = xP_{pub} - rS_{ID_a}$, 最后发送 $\sigma = (c, r, S)$.

解密验证：给定 ID_a, S_{ID_b}, σ, 计算 $Q_{ID_a} = H_1(ID_a)$. 分段 $\sigma = (c, r, S)$, 计算 $k_1 = e(P, S)e(P_{pub}, Q_{ID_a})^r$, $t = e(S, Q_{ID_b})e(Q_{ID_a}, S_{ID_b})^r$, $r = H_2(t), m = D_{k_2}(c)$, 验证是否 $r = H_3(c, k_1)$.

在 DBDH 问题难解的假设下, 该方案在 Random Oracle 模型下是可证明安全的.

上述各种方案都可以给出严格的形式化安全定义, 并在 Random Oracle 模型和相应的难解性假设下可证明是满足这些安全性定义的, 为了避免引入过多的复杂的形式化定义和证明, 这里只是简单给出方案描述及其安全性结论, 如需详细了解可参阅文中给出的相关文献. 上面所述的几种方案只是基于双线性对的最具代表性的情形. 总而言之, 基于双线性对相关的难题, 我们不仅可以方便地构造基本密码方

案：加密、签名、密钥协商，也可以构造其他特殊的密码方案：签密、门限解密、密钥共享、身份认证、无常 Hash(Chameleon Hash) 等. 特别值得一提的是，正是基于双线性对的若干性质，人们才提出了适合应用的基于身份的密码方案和一轮三方密钥协商协议.

第二部分

提升到整体域上的点数计算算法

第二章　复数域上的椭圆曲线

§2.1　Weierstrass $\wp$ 函数和椭圆曲线

设 ω_1 和 ω_2 为两个复数, 且 $\omega_1/\omega_2 \in \mathfrak{H} = \{z \in \mathbb{C} | \mathrm{Im}(z) > 0\}$(上半平面). 这里 $\mathbb{C}$ 表示复数域. 集合 $L = \{a\omega_1 + b\omega_2 | a, b \in \mathbb{Z}\}$($\mathbb{Z}$ 为整数集合) 称为一个格, ω_1 和 ω_2 是 L 的基. $\mathbb{C}$ 上的亚纯函数 $f(z)$ 称为 (L 上的) 椭圆函数, 如果它以格 L 为周期, 即

$$f(z+\omega) = f(z), \quad \forall \omega \in L,\ z \in \mathbb{C}.$$

显然 $f(z)$ 以 L 为周期, 当且仅当

$$f(z+\omega_1) = f(z+\omega_2) = f(z).$$

L 上的所有椭圆函数构成一个域, 记为 $\mathbb{C}(L)$. L 上的椭圆函数由它在 $\mathbb{C}/L = \{t_1\omega_1 + t_2\omega_2 | 0 \leqslant t_i < 1\}$ 上的局限所决定, 所以也可看成是 $\mathbb{C}/L$ 上的函数.

有界整函数必定是常数 (Liouville 定理), 所以椭圆整函数必定是常数, 这是因为它在 $\{t_1\omega_1 + t_2\omega_2 | 0 \leqslant t_i \leqslant 1\}$ 上是连续的, 因而是有界的.

定理 2.1　格 L 上非常值的椭圆函数 $f(z)$ 有如下性质:

(i) $\sum_{\omega \in \mathbb{C} \setminus L} \mathrm{res}_w(f) = 0$,

(ii) $\sum_{\omega \in \mathbb{C} \setminus L} \mathrm{ord}_w(f) = 0$,

(iii) $\sum_{\omega \in \mathbb{C} \setminus L} \mathrm{ord}_w(f) w \in L$,

这里 $\mathrm{res}_\omega(f)$ 表示 f 在 ω 的残数, $\mathrm{ord}_\omega(f)$ 表示 f 在 ω 的阶 (当 ω 为 f 的零点时, $\mathrm{ord}_\omega(f)$ 为正数, ω 为 f 的极点时, $\mathrm{ord}_\omega(f)$ 为负数).

证明　取平等四边形 P, 由于 $f(z)$ 是亚纯函数, 适当选取 α, 可认为 $f(z)$ 在 P 的边界 ∂P 上没有零点, 也没有极点, 见图 2.1.

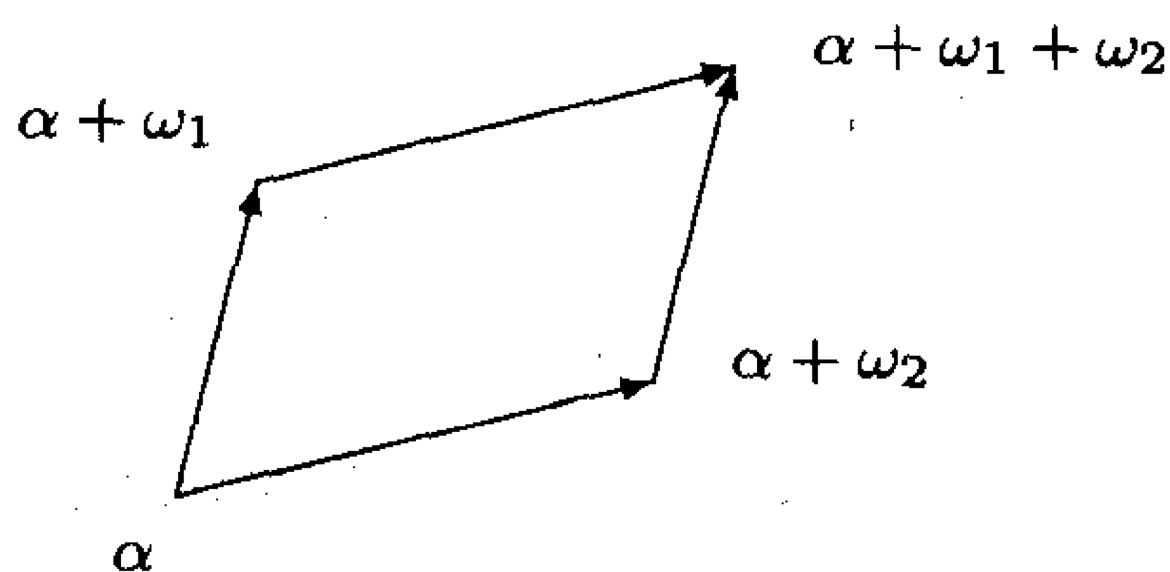


图 2.1　格的基本平行四边形

(i) 我们有

$$
\begin{aligned}
&2\pi i \sum_{\omega\in\mathbb{C}/L} \mathrm{res}_\omega(f)\\
&= 2\pi i \sum_{\omega\in P} \mathrm{res}_\omega(f) = \int_{\partial P} f(z)dz\\
&= \int_\alpha^{\alpha+\omega_2} f(z)dz + \int_{\alpha+\omega_2}^{\omega+\omega_1+\omega_2} f(z)dz + \int_{\alpha+\omega_1+\omega_2}^{\alpha+\omega_1} f(z)dz + \int_{\alpha+\omega_1}^{\alpha} f(z)dz\\
&= \int_\alpha^{\alpha+\omega_2} f(z)dz + \int_\alpha^{\alpha+\omega_1} f(z)dz - \int_\alpha^{\alpha+\omega_2} f(z)dz - \int_\alpha^{\alpha+\omega_1} f(z)dz\\
&= 0.
\end{aligned}
$$

(ii) $f'(z)/f(z)$ 也是 L 上的椭圆函数, 易见 $\mathrm{res}_\omega(f'/f) = \mathrm{ord}_\omega(f)$, 所以

$$
0 = \int_{\partial P} f'(z)/f(z)dz = 2\pi i \sum_{\omega\in P} \mathrm{res}_\omega(f'/f) = 2\pi i \sum_{\omega\in\mathbb{C}/L} \mathrm{ord}_\omega(f).
$$

(iii) 我们有

$$
\int_{\partial P} z\frac{f'(z)}{f(z)}dz = 2\pi i \sum_{\omega\in P} \mathrm{res}_\omega\left(z\frac{f'(z)}{f(z)}\right) = 2\pi i \sum_{\omega\in\mathbb{C}/L} \mathrm{ord}_\omega(f)\omega.
$$

计算在 P 的两条相对的边上的积分

$$
\begin{aligned}
\int_\alpha^{\alpha+\omega_1} z\frac{f'(z)}{f(z)}dz - \int_{\alpha+\omega_2}^{\alpha+\omega_2+\omega_1} z\frac{f'(z)}{f(z)}dz &= -\omega_2 \int_\alpha^{\alpha+\omega_1} \frac{f'(z)}{f(z)}dz\\
&= -\omega_2 \log f(z)\Big|_\alpha^{\alpha+\omega_1} = 2\pi i k\omega_2,
\end{aligned}
$$

这里 k 为整数, 同样计算 P 的另外两条相对边上的积分, 证得 (iii), 证毕.

定义 2.1　设 L 为一格, 定义与格 L 相关的Wereistrass $\wp$ 函数为

$$
\wp(z,L) = \frac{1}{z^2} + \sum_{w\in L'} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right),
$$

其中求和符号是对格 L 中的所有非零元素求和.

Wereistrass $\wp$ 函数有如下性质:

(1) Wereistrass $\wp$ 函数在不包含格 L 中的点的任意紧子集上都一致收敛;

(2) $\wp(z,L)$ 的极点是格 L 中的点, 没有其他极点, 并且所有的极点都是 2 阶极点;

(3) $\wp(z,L)$ 是 L 周期的.

因此, Wereistrass $\wp$ 函数是一个椭圆函数. 性质 (3) 的证明如下: $\wp(z,L)$ 是偶函数, 这是显然的; 其次, 对 $\wp(z,L)$ 求导得

$$\wp'(z,L) = -2\sum_{\omega\in L}\frac{1}{(z-\omega)^3},$$

这里是对格 L 中的所有点求和. 显然 $\wp'(z,L)$ 是 L 周期的, 并且是奇函数, 即

$$\wp'(-z,L) = -\wp'(z,L), \qquad \wp'(z,L) = \wp'(z+\omega,L),\ \forall\,\omega\in L$$

对上面第二式两边积分, 可知存在一个常数 C, 使得

$$\wp(z,L) = \wp(z+\omega_1,L) + C.$$

令 $z = -\omega_1/2$ 代入上式可得

$$\wp(-\omega_1/2,L) = \wp(\omega_1/2,L) + C.$$

由于 $\wp(z,L)$ 是偶函数, 所以 $C=0$, 即 $\wp(z+\omega_1,L) = \wp(z,L)$; 同样可证 $\wp(z+\omega_2,L) = \wp(z,L)$, 因此 $\wp(z,L)$ 是 L 周期的.

易见 $\wp'(z,L)$ 也是 L 周期的. 在不会引起混淆时, 记 $\wp(z,L)=\wp(z)$, $\wp'(z,L) = \wp'(z)$.

定理 2.2 格 L 上的所有椭圆函数构成的域 $\mathbb{C}(L)$ 是由 $\wp(z,L)$ 和 $\wp'(z,L)$ 生成的, 换句话说, L 上的任一椭圆函数可表为 $\wp(z)$ 和 $\wp'(z)$ 的有理函数.

证明 由 $\wp$ 函数的定义可知 $\wp(z)=\wp(-z)$, 即 $\wp(z)$ 是偶函数. $\wp'(z)$ 是奇函数, 即 $\wp'(-z) = -\wp'(z)$. 设 $f(z)$ 是 L 上的任一椭圆函数, 由于

$$f(z) = \frac{f(z)+f(-z)}{2} + \frac{f(z)-f(-z)}{2},$$

f 表为一个偶函数和一个奇函数之和. 当 f 为奇函数时, $f\wp'$ 即为偶函数. 所以仅需证明当 f 为偶函数时, f 可表为 $\wp$ 的有理函数 (即 $f\in\mathbb{C}(\wp)$) 即可.

设 $f(z)$ 在 u 点有 m 阶零点, 若 $-u\not\equiv u \pmod L$, 则 $f(z)$ 在 $-u$ 点也有 m 阶零点, 这是因为 $f^{(k)}(u) = (-1)^k f^{(k)}(-u)$. 若 $-u\equiv u \pmod L$, 则 m 一定是偶数. 由于 $2u\in L$, 在 $\mathbb{C}/L$ 中 u 仅可能为

$$0,\ \frac{\omega_1}{2},\ \frac{\omega_2}{2},\ \frac{\omega_1+\omega_2}{2}.$$

f 为偶函数, f' 为奇函数, 则 $f'(u) = f'(-u) = -f'(u)$, 所以 $f'(u)=0$, f 在 u 点至少有 2 阶零点, 当 $u\notin L$ 时, 将上述推论用于函数

$$g(z) = \wp(z) - \wp(u),$$

可知 $g(z)$ 在 u 点至少有一个 2 阶零点, 但由于 $g(z)$ 在 $\mathbb{C}/L$ 中仅有一个 2 阶极点 $z=0$, 利用定理 2.1 的 (ii), u 是 $g(z)$ 的二阶零点. 如果 $f(u)/g(u)\neq 0$, 则 $\mathrm{ord}_u(f)=2$; 如果 $f(u)/g(u)=0$, 则 f/g 在 u 点的阶至少为 2. 重复上述推论, 最后可以证明 m 为偶数. 当 $u\in L$ 时, 以 $g=1/\wp$ 代替上述 g, 同样可以证明 m 为偶数.

若 $f(z)$ 在 u 点有 m 阶极点, 以 $1/f$ 代替 f, 利用上述同样方法可以证明当 $u\not\equiv -u \pmod L$ 时, $f(z)$ 在 $-u$ 点也有 m 阶极点; 当 $2u\equiv 0 \pmod L$ 时, m 一定是偶数.

设 $(u_i,-u_i) \pmod L\,(i=1,2,\cdots,r)$ 跑遍 $f(z)$ 所有零点和极点, 且 $u_i\notin L\,(i=1,2,\cdots,r)$, 令

$$\begin{aligned} m_i &= \mathrm{ord}_{u_i}f, && \text{若 } 2u_i\not\equiv 0 \pmod L,\\ m_i &= \frac{1}{2}\mathrm{ord}_{u_i}f, && \text{若 } 2u_i\equiv 0 \pmod L. \end{aligned}$$

上述推导同样也证明了对任一 $\alpha\in\mathbb{C}$, $\alpha\notin L$, 当 $2\alpha\not\equiv 0 \pmod L$ 时, $\wp(z)-\wp(\alpha)$ 在 α 和 $-\alpha$ 各有一个一阶零点; 当 $2\alpha\equiv 0 \pmod L$ 时, $\wp(z)-\wp(\alpha)$ 在 α 点有一个 2 阶零点. 可见对任一 $z\not\equiv 0 \pmod L$ 时, 乘积

$$\prod_{i=1}^{r}\left(\wp(z)-\wp(u_i)\right)^{m_i}$$

与 f 在 z 点有同样的阶. 利用定理 2.1 的 (ii), 可知 f 与上述乘积在 $z\in L$ 点也有同样的阶, 所以该乘积与 f 的商既没有零点, 也没有极点, 由 Liouville 定理, 该商为一个非零常数, 定理 2.2 证毕.

计算 $\wp(z,L)$, $\wp'(z,L)$ 的幂级数展开式

$$\begin{aligned} \wp(z,L) &= \frac{1}{z^2}+\sum_{\omega\in L'}\left[\frac{1}{\omega^2}\left(1+\frac{z}{\omega}+\left(\frac{z}{\omega}\right)^2+\cdots\right)^2-\frac{1}{\omega^2}\right]\\ &= \frac{1}{z^2}+\sum_{\omega\in L'}\sum_{m=1}^{\infty}(m+1)\left(\frac{z}{\omega}\right)^m\cdot\frac{1}{\omega^2}\\ &= \frac{1}{z^2}+\sum_{m=1}^{\infty}c_m z^m, \end{aligned}$$

其中

$$c_m=\sum_{\omega\in L'}\frac{m+1}{\omega^{m+2}}.$$

当 m 为奇数时 $c_m=0$. 定义

$$s_m(L)=s_m=\sum_{\omega\in L'}\frac{1}{\omega^m},$$

则有

$$\wp(z)=\frac{1}{z^2}+\sum_{n=1}^{\infty}(2n+1)s_{2n+2}(L)z^{2n}=\frac{1}{z^2}+3s_4z^2+5s_6z^4+\cdots,$$

以及

$$\wp'(z)=\frac{-2}{z^3}+\sum_{n=1}^{\infty}2n(2n+1)s_{2n+2}z^{2n-1}=\frac{-2}{z^3}+6s_4z+20s_6z^3+\cdots.$$

计算 $\wp'(z)^2$ 及 $\wp(z)^3$:

$$\wp(z)^3=\frac{1}{z^6}+\frac{9s_4}{z^2}+15s_6+\cdots,$$

$$\wp'(z)^2=\frac{4}{z^6}-\frac{24s_4}{z^2}-80s_6+\cdots.$$

易见在 $\wp'^2-4\wp^3+60s_4\wp+140s_6$ 的幂级数展开式中没有 z 的负幂次项, 常数项也为零, 利用 Liouille 定理, 可知该椭圆函数恒为零. 令 $g_2=g_2(L)=60s_4$, $g_3=g_3(L)=140s_6$, 则

$$\wp'^2=4\wp^3-g_2\wp-g_3.$$

这表示当 $z\notin L$ 时, 它对应曲线

$$y^2=4x^3-g_2x-g_3 \tag{2.1}$$

上的一个点 $(\wp(z),\wp'(z))$. 我们把方程 (2.1) 所定义的曲线称为椭圆曲线. 由于 $\wp(z)$ 和 $\wp'(z)$ 都是 L 上的椭圆函数, 实际上这表示 $\mathbb{C}/L$ 中每个非零点 $z+L\,(z\notin L)$ 对应曲线 (2.1) 上的一个点 $(\wp(z),\wp'(z))$. 这里将 $\mathbb{C}$ 看作一个加法群, L 是它的加法子群.

上述由 $\mathbb{C}/L$ 到曲线 (2.1) 的映射是映上的. 令 x 取任一复数 a, 若 a 不是 $4x^3-g_2x-g_3$ 的根, 则 a 决定曲线 (2.1) 上两个点 (a,b) 和 $(a,-b)$, 这里 $b^2=4a^3-g_2a-g_3$; 若 $4a^3-g_2a-g_3=0$, 则 a 决定曲线 (2.1) 上 1 个点 $(a,0)$. 另一方面, 在定理 2.2 的证明中, 已知 $\wp(z)-a$ 或有 2 个 1 阶零点 $u,-u \pmod L$, 或有 1 个 2 阶零点 u, 前一情形, a 决定曲线 (2.1) 上的两个点 $(\wp(u),\wp'(u))$, $(\wp(u),-\wp'(u))$, 后一情形, a 决定曲线 (2.1) 上的 1 个点 $(\wp(u),0)$. 所以上述定义的映射是映上的.

为了使 $\mathbb{C}/L$ 中的零点也能对应曲线 (2.1) 上的 1 个点, 我们将 $\mathbb{C}$ 上的仿射平面扩充为 $\mathbb{C}$ 上的射影平面. $\mathbb{C}$ 上的仿射平面上任一点表为 $(x,y)\,(x,y\in\mathbb{C})$, $\mathbb{C}$ 上的射影平面上任一点为 $(x,y,z)\,(x,y,z\in\mathbb{C}$, x,y,z不能同时为零), 且对任一非零

$\lambda \in \mathbb{C}$, $\lambda(x,y,z)$ 与 (x,y,z) 视为同一点. 当 $z \neq 0$ 时, 在射影平面上的点 $(x,y,z) = (x/z, y/z, 1)$, 它对应仿射平面上的一个点 $(x/z, y/z)$. 仿射平面上曲线 (2.1) 对应射影平面上的曲线

$$E: \ y^2 z = 4x^3 - g_2 x z^2 - g_3 z^3, \tag{2.2}$$

曲线 E 称为曲线 (2.1) 的齐次化, 当 $z = 1$ 时, 曲线 (2.2) 即为曲线 (2.1). 当 $z = 0$ 时, 有惟一的点 $(0,1,0)$ 在曲线 E 之上. 所以曲线 E 比曲线 (2.1) 多了 1 个点 $(0,1,0)$, 通常称该点为无穷远点, 记为 $\mathcal{O} = (0,1,0)$. 因而可以将 $\mathbb{C}/L$ 的零点对应到点 $\mathcal{O}$.

$\mathbb{C}/L$ 是一个加法群, 既然 $\mathbb{C}/L$ 中的点都对应 E 上的点, 则可以把 $\mathbb{C}/L$ 上的加法移植到 E 上, 即在 E 上也定义相应的加法. $\mathcal{O}$ 将成为 E 的加法的零点.

首先, $(\wp(u), \wp'(u))$ 与 $(\wp(-u), \wp'(-u)) = (\wp(u), -\wp'(u))$ 相加得 $\mathcal{O}$. 设 $u_1, u_2 \notin L$, 且 $u_1 \pm u_2 \notin L$, 记

$$\begin{aligned}
P_1 &= (x_1, y_1) = (\wp(u_1), \wp'(u_1)), \\
P_2 &= (x_2, y_2) = (\wp(u_2), \wp'(u_2)), \\
P_3 &= (x_3, y_3) = (\wp(u_1 + u_2), \wp'(u_1 + u_2)).
\end{aligned}$$

我们有 $P_3 = P_1 + P_2$, 这里的加法是椭圆曲线 E 上的加法. 下面证明 x_3, y_3 是 x_1, y_1, x_2, y_2 的有理函数. 设 $y = ax + b$ 是通过 P_1 和 P_2 的直线, 因而

$$\wp'(u_1) = a\wp(u_1) + b, \qquad \wp'(u_2) = a\wp(u_2) + b, \tag{2.3}$$

可见 u_1 和 u_2 是椭圆函数 $\wp'(z) - a\wp(z) - b$ 的两个零点. 该函数有惟一的 3 阶极点 $z \equiv 0 \pmod L$, 由定理 2.1 的 (ii), 它也有 3 个零点. 记除 u_1, u_2 之外的第三个零点为 u_3, 假设 u_1, u_2, u_3 都是 1 阶零点, 由定理 2.1 的 (iii) 可得

$$u_3 \equiv -(u_1 + u_2) \pmod L,$$

因此也有

$$\wp'(u_3) = a\wp(u_3) + b.$$

方程

$$4x^3 - g_2 x - g_3 - (ax + b)^2 = 0$$

有 3 个根 $\wp(u_1)$, $\wp(u_2)$, $\wp(u_3)$, 上式左端可分解为

$$4(x - \wp(u_1))(x - \wp(u_2))(x - \wp(u_3)),$$

比较 x^2 的系数得到

$$\wp(u_1)+\wp(u_2)+\wp(u_3)=\frac{a^2}{4}.$$

由 (2.3) 式可得

$$a\big(\wp(u_1)-\wp(u_2)\big)=\wp'(u_1)-\wp'(u_2).$$

由于

$$\wp(u_3)=\wp\big(-(u_1+u_2)\big)=\wp(u_1+u_2),$$

所以

$$\wp(u_1+u_2)=-\wp(u_1)-\wp(u_2)+\frac{1}{4}\Big(\frac{\wp'(u_1)-\wp'(u_2)}{\wp(u_1)-\wp(u_2)}\Big)^2. \tag{2.4}$$

易见

$$\wp'(u_1+u_2)=\big(\wp(u_1)-\wp(u_1+u_2)\big)a-\wp'(u_1).$$

在 (2.4) 式中令 $u_1\to u_2=u$, 并设 $\wp'(u)\neq 0$, 得到 (利用 $\wp''(u)=(12\wp(u)^2-g_2)/2$)

$$\wp(2u)=-2\wp(u)+\frac{1}{4}\Big(\frac{\wp''(u)}{\wp'(u)}\Big)^2=-2\wp(u)+\frac{1}{4}\Big(\frac{12\wp^2(u)-g_2}{2\wp'(u)}\Big)^2.$$

将上式求微商可得到 (利用 $\wp'''(u)=12\wp(u)\wp'(u)$)

$$\begin{aligned}2\wp'(2u)&=-2\wp'(u)+\frac{1}{2}\cdot\frac{\wp''(u)}{\wp'(u)}\cdot\frac{\wp'''(u)\wp'(u)-\big(\wp''(u)\big)^2}{\big(\wp'(u)\big)^2}\\&=-2\wp'(u)+2\frac{\wp''(u)}{\wp'(u)}\big(\wp(u)-\wp(2u)\big),\end{aligned}$$

即

$$\wp'(2u)=\big(\wp(u)-\wp(2u)\big)\Big(\frac{12\wp^2(u)-g_2}{2\wp'(u)}\Big)-\wp'(u).$$

椭圆曲线 E 上的加法规则可以归纳如下：

(1) E 上任一点 P, 有 $P+\mathcal{O}=P$;

(2) $P=(x,y)$, 则 $-P=(x,-y)$, 即 $(x,y)+(x,-y)=\mathcal{O}$;

(3) 设 $P_1=(x_1,y_2)$, $P_2=(x_2,y_2)$, $P_3=P_1+P_2=(x_3,y_3)$, 且 $P_1\neq\pm P_2$, 这时一定有 $x_1\neq x_2$. 令 $\lambda=\frac{y_1-y_2}{x_1-x_2}$, 则

$$x_3=-x_1-x_2+\frac{\lambda^2}{4},\quad y_3=\lambda(x_1-x_3)-y_1.$$

(4) 设 $P_1=(x_1,y_1)$, $P_1\neq -P_1$, $P_3=2P_1=(x_3,y_3)$, 这时 $y_1\neq 0$, 令 $\lambda=\frac{12x_1^2-g_2}{2y_1}$, 则

$$x_3=-2x_1+\frac{\lambda^2}{4},\quad y_3=\lambda(x_1-x_3)-y_1.$$

综合上述讨论, 得到以下定理:

定理 2.3　设 L 为 $\mathbb{C}$ 中的格, E 为由方程

$$y^2=4x^3-g_2(L)x-g_3(L)$$

定义的椭圆曲线, 则映射

$$\begin{aligned}\varphi:\ \ &\mathbb{C}/L \longrightarrow E\\ &z \longmapsto (\wp(z),\wp'(z)),\quad z\notin L\\ &0 \longmapsto \mathcal{O}\end{aligned}$$

是同构映射.

§2.2　椭圆曲线的同构

设 M 和 L 为 $\mathbb{C}$ 中的两个格, 若存在复数 $c\neq 0$, 使得 $M=cL$, 则称格 L 与 M 等价, 这时

$$\begin{aligned}\gamma:\ \ &\mathbb{C}/L \longrightarrow \mathbb{C}/M\\ &z \longmapsto cz\end{aligned}$$

是一个同构映射, 显然 γ 也是复解析的. 由定理 2.3, $\mathbb{C}/L$ 和 $\mathbb{C}/M$ 分别与椭圆曲线

$$A:\quad y^2=4x^3-g_2(L)x-g_3(L)$$

和

$$B:\quad y^2=4x^3-g_2(M)x-g_3(M)$$

同构, 因而 γ 可以诱导 A 与 B 之间的一个同构 λ:

$$\begin{array}{ccc}\mathbb{C}/L & \xrightarrow{\ \gamma\ } & \mathbb{C}/M\\ {\scriptstyle\varphi}\big\downarrow & & \big\downarrow{\scriptstyle\psi}\\ A & \xrightarrow[\ \lambda\ ]{} & B\end{array}$$

这里

$$\varphi(z) = \big(\wp(z, L),\, \wp'(z, L)\big), \qquad z \in \mathbb{C}/L,$$
$$\psi(z) = \big(\wp(z, M),\, \wp'(z, M)\big), \qquad z \in \mathbb{C}/M,$$

易见

$$\begin{aligned}\lambda\big(\wp(z, L),\, \wp'(z, L)\big) &= \big(\wp(cz,\, M),\, \wp'(cz,\, M)\big)\\ &= \big(\wp(cz,\, cL),\, \wp'(cz,\, cL)\big)\\ &= \big(c^{-2}\wp(z, L),\, c^{-3}\wp'(z, L)\big),\end{aligned}$$

换句话说, 若 $\lambda(x, y) = (x', y')$ $\big((x, y) \in A,\ (x', y') \in B\big)$, 则 $x' = -c^2 x$, $y' = -c^3 y$. 这时定义 A 和 B 的方程中的系数也有关系: $g_2(M) = c^{-4} g_2(L)$, $g_3(M) = c^{-6} g_2(L)$.

反之, 若 $\lambda(x, y) = (x', y')$ 是 A 与 B 之间的 (群) 同构映射, 且是复解析映射, 则 λ 也可以诱导 $\mathbb{C}/L$ 与 $\mathbb{C}/M$ 之间的一个解析同构.

命题 2.1 设 L 和 M 是 $\mathbb{C}$ 中的两个格,

$$\lambda: \quad \mathbb{C}/L \longrightarrow \mathbb{C}/M$$

是复解析的同态, 则存在复数 c, 使得下列图可交换:

$$\begin{array}{ccc}\mathbb{C} & \xrightarrow{\ c\ } & \mathbb{C}\\ \big\downarrow & & \big\downarrow\\ \mathbb{C}/L & \xrightarrow[\lambda]{} & \mathbb{C}/M\end{array}$$

上端映射为 $z \mapsto cz$, 两侧的映射分别为 $z \mapsto z \pmod L$ 和 $z \mapsto z \pmod M$.

证明 λ 可扩展为一个解析映射 $f: \mathbb{C} \to \mathbb{C}$, $f(0) = 0$, 且使下列图可交换:

$$\begin{array}{ccc}\mathbb{C} & \xrightarrow{\ f\ } & \mathbb{C}\\ \big\downarrow & & \big\downarrow\\ \mathbb{C}/L & \xrightarrow[\lambda]{} & \mathbb{C}/M\end{array}$$

对任一 $\omega \in L$, $f(z + \omega) = f(z) \pmod M$ 对所有 $z \in \mathbb{C}$ 成立. 由于 M 是离散的, $f(z+\omega) - f(z)$ 是 z 的连续函数, 所以 $f(z+\omega) - f(z)$ 是一个不依赖 z 的常数, 从而对所有 $z \in \mathbb{C}$, $\omega \in M$ 有 $f'(z + \omega) = f'(z)$, f' 是一个 $\mathbb{C}$ 上解析的椭圆函数, 必定为一常数, 因而 $f(z) = cz + d$, 由 $f(0) = 0$ 得 $d = 0$, 证毕.

命题 2.1 确定了 A 和 B 之间的所有 (复解析) 同构.

定义

$$J(L) = \frac{g_2^3(L)}{g_2^3(L) - 27 g_3^2(L)}, \quad J(M) = \frac{g_2^3(M)}{g_2^3(M) - 27 g_3^2(M)},$$

当 A 与 B 同构时, 一定存在 $c \neq 0$, 使得 $M = cL$, 因而 $J(L) = J(M)$. 以下将证明若 $J(L) = J(M)$, 则 A 与 B 同构. 我们把 $J(L)$ 称为椭圆曲线 A 的 j 不变量.

$J(L)$ 的分母 $\Delta(L) = g_2^3(L) - 27g_3^2(L)$ 称为椭圆曲线 A 的判别式, 它恒不为零.

命题 2.2　$\Delta(L) \neq 0$.

证明　$\Delta(L)$ 是 3 次多项式 $f(x) = 4x^3 - g_2(L)x - g_3(L)$ 的判别式, 仅需证明 $f(x)$ 没有重根. 由于

$$\wp'\left(\frac{\omega_1}{2}\right) = \wp'\left(\frac{\omega_2}{2}\right) = \wp'\left(\frac{\omega_1 + \omega_2}{2}\right) = 0,$$

所以 $e_1 = \wp\left(\frac{\omega_1}{2}\right)$, $e_2 = \wp\left(\frac{\omega_2}{2}\right)$, $e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$ 是 $f(x)$ 的 3 个根. 函数 $h(z) = \wp(z) - e_1$ 在 $\mathbb{C}/L$ 上仅有一个 2 阶极点, 因而有 2 个零点. 易见 $z = \frac{\omega_1}{2}$ 是 h 的 2 阶零点, h 在 $\mathbb{C}/L$ 上不再有其他零点, 因而 $h(\omega_2/2) = e_2 - e_1 \neq 0$, $h\left(\frac{\omega_1+\omega_2}{2}\right) = e_3 - e_1 \neq 0$. 类似地可以证明 $e_2 \neq e_3$, 证毕.

设

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

为行列式大于零的实矩阵, τ 为上半平面 $\mathfrak{H}$ 中任一点, 由于

$$\operatorname{Im} \frac{a\tau + b}{c\tau + d} = \frac{(ad - bc)\operatorname{Im}(z)}{|c\tau + d|^2},$$

所以

$$\tau \longmapsto \alpha(\tau) = \frac{a\tau + b}{c\tau + d}$$

为 $\mathfrak{H}$ 上的一个变换, 设 $f(\tau)$ 为定义在 $\mathfrak{H}$ 上的函数, 定义

$$(f \circ \alpha)(\tau) = f(\alpha(\tau)).$$

令

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \left(\begin{array}{cc} a & b \\ c & d \end{array} \right) \middle| \, ad - bc = 1,\ a, b, c, d \in \mathbb{Z} \right\},$$

$\mathrm{SL}_2(\mathbb{Z})$ 称为模群.

设 k 为非负整数, f 为定义在 $\mathfrak{H}$ 上的函数, 若 f 适合下列条件:

(1) f 为 $\mathfrak{H}$ 上的亚纯函数;

(2) 对任一 $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, 有 $f(\alpha(\tau)) = (c\tau + d)^{2k} f(\tau)$;

(3) f 在 ∞ 亚纯, 即有展开式 $f(z) = \sum_{n=-N}^{\infty} c_n q^n$ (这里 $q = e^{2\pi i\tau}$).

则 f 称为 ($\mathrm{SL}_2(\mathbb{Z})$ 上) 权为 $2k$ 的模形式, 当 $k = 0$ 时 f 亦称为 ($\mathrm{SL}_2(\mathbb{Z})$ 上) 模函数 (亦可以对模群的任一子群 Γ 定义模形式, 这时条件 (3) 改为 f 在 Γ 的任一尖点是亚纯的, 参见文献 [10]).

在性质 (2) 中, 取 $\alpha = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$, 可得 $f(\tau + 1) = f(\tau)$, 所以 $f(\tau)$ 可展开为 q 的幂级数. 性质 (3) 是说该展开式中仅有有限个 q 的负幂次项. $-N$ 称为 f 在 ∞ 的阶, 记为 $\mathrm{ord}_\infty(f)$.

Eisenstein 级数 ($k > 1$) $G_k(\tau) = \sum{}'_{m,n} \frac{1}{(m\tau+n)^{2k}}$ 是一类重要的权为 $2k$ 的模形式, 求和号中 m 和 n 不同时为零. $G_k(\tau)$ 是 $\mathfrak{H}$ 上的全纯函数. 我们有 G_k 的 q 展开式 [10]

$$G_k(\tau) = 2\zeta(2k) + 2 \cdot \frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n, \tag{2.5}$$

其中 $\sigma_k(n) = \sum_{d|n} d^k$.

设 τ_1 和 τ_2 为格 L 的基, $\tau = \tau_1/\tau_2 \in \mathfrak{H}$, 记 $L = \mathbb{Z}\tau_1 + \mathbb{Z}\tau_2 = \tau_2(\mathbb{Z} + \mathbb{Z}_\tau)$, 令

$$j(L) = 1728 \cdot \frac{g_2^3(L)}{g_2^3(L) - 27 g_3^2(L)} \tag{2.6}$$

(这里取系数 $1728 = 3^3 \cdot 2^6$ 是为了使 j 的 q 展开式首项系数为 1). 由于 $j(cL) = j(L)\,(c \neq 0)$, $j(L)$ 可表为 τ 的函数 $j(\tau)$, $j(\tau)$ 是 $\mathfrak{H}$ 上的全纯函数 (命题 2.2).

设 $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(\mathbb{Z})$, 易见 $a\tau_1 + b\tau_2$, $c\tau_1 + d\tau_2$ 也是 L 的一组基, 即

$$L = \mathbb{Z}_{a\tau_1 + b\tau_2} + \mathbb{Z}_{c\tau_1 + d\tau_2} = (c\tau_1 + d\tau_2)(\mathbb{Z}_1 + \mathbb{Z}_{\tau'})$$

其中

$$\tau' = \frac{a\tau + b}{c\tau + d},$$

所以

$$j(\alpha(\tau)) = j(\tau') = j(\tau), \qquad \forall \alpha \in \mathrm{SL}_2(\mathbb{Z}).$$

下面计算 $j(\tau)$ 的 q 展开式. 已知

$$\zeta(4) = \frac{\pi^4}{90}, \quad \zeta(6) = \frac{\pi^6}{945},$$

利用 (2.5) 式可得

$$\begin{aligned} g_2(\tau) &= 60G_2(\tau) = 60\left(\frac{2\pi^4}{90} + \frac{(2\pi)^4}{3}\sum_{n=1}^{\infty}\sigma_3(n)q^n\right) \\ &= \frac{(2\pi)^4}{12}\left(1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right), \\ g_3(\tau) &= 140G_3(\tau) = 140\left(\frac{2\pi^6}{945} - \frac{(2\pi)^6}{60}\sum_{n=1}^{\infty}\sigma_5(n)q^n\right) \\ &= \frac{(2\pi)^6}{6^3}\left(1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n\right). \end{aligned} \tag{2.7}$$

令

$$E_4(\tau) = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n = 1 + 240X,$$

$$E_6(\tau) = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n = 1 - 504Y,$$

则

$$\begin{aligned} \Delta = g_2^3 - 27g_3^2 &= (2\pi)^{12}\cdot\frac{E_4(\tau)^3 - E_6^2(\tau)}{2^6\cdot 3^3} \\ &= \frac{(2\pi)^{12}}{2^6\cdot 3^3}\left[(1+240X)^3 - (1-504Y)^2\right]. \end{aligned}$$

上述方括号中的 q 展开式每个系数都是 $2^6\cdot 3^3 = 1728$ 的倍数, 这是因为

$$(1+240X)^3 - (1-504Y)^2 \equiv 3^2\cdot 2^4(5X+7Y) \pmod{2^6\cdot 3^3}$$

对任一正整数 d, 有 $d^3 \equiv d^5 \pmod{12}$, 故对任一 n 有

$$\sum_{d|n} d^3 \equiv \sum_{d|n} d^5 \pmod{12},$$

所以

$$\Delta = (2\pi)^{12}q\left(1 + \sum_{n=1}^{\infty}d_n q^n\right),$$

其中 d_n 为整数. 从而

$$\begin{aligned} j = (12)^3\frac{g_2^3}{\Delta} &= \frac{1728E_4^3(\tau)}{E_4^3(\tau) - E_6^2(\tau)} = \frac{1}{q} + \sum_{n=0}^{\infty}a_n q^n \\ &= \frac{1}{q} + 744 + 196884q + \cdots. \end{aligned} \tag{2.8}$$

综上所述, 可知 $j(\tau)$ 是模函数, 且 ∞ 是 $j(\tau)$ 的 1 阶极点.

记 $\Gamma = \mathrm{SL}_2(\mathbb{Z})$, 令

$$D = \left\{\tau \in \mathfrak{H} \,\middle|\, \frac{1}{2} \leqslant \mathrm{Re}(\tau) \leqslant \frac{1}{2}, |\tau| \geqslant 1\right\},$$

则称 D 为 Γ 在 $\mathfrak{H}$ 中的基域, 即 Γ 在 $\mathfrak{H}$ 中的任一轨道至少有 1 个点在 D 中, 且 D 中任意两点若在同一轨道上, 则它们一定在 D 的边界上.

命题 2.3 *设 $f(\tau)$ 是权为 $2k$ 的模形式, $f \neq 0$, 则*

$$\mathrm{ord}_\infty(f) + \frac{1}{3}\mathrm{ord}_\rho(f) + \frac{1}{2}\mathrm{ord}_i(f) + \sum_{P \neq i,\rho} \mathrm{ord}_P(f) = \frac{k}{6}. \tag{2.9}$$

求和号跑遍 D 中除了 i 和 $\rho = e^{2\pi i/3}$ 之外的所有点.

证明 利用 D 的边界上的围道积分可证明 [11], 证毕.

定理 2.4 *映射 $j : \Gamma \setminus \mathfrak{H} \to \mathbb{C}$ 是双射.*

证明 我们即要证明对任一 $c \in \mathbb{C}$, 存在惟一的 $\tau_0 \in \Gamma \setminus \mathfrak{H}$, 使得 $j(\tau_0) = c$. 令 $f(\tau) = j(\tau) - c$, 它是模函数, 在 $\mathfrak{H}$ 上全纯, 且 $\mathrm{ord}_\infty(f) = -1$, 由命题 2.3 得 $(k = 0)$

$$\frac{1}{3}\mathrm{ord}_\rho(f) + \frac{1}{2}\mathrm{ord}_i(f) + \sum_{P \neq i,\rho} \mathrm{ord}_P(f) = 1,$$

上式左端各项都是正的, 故 $f(\tau)$ 只能在 $\Gamma \setminus \mathfrak{H}$ 中惟一的点 z_0 上有正的阶. 当 z_0 与 i 或 ρ 不在同一轨道上时, f 在 z_0 的阶为 1, 否则 f 在 ρ 的阶为 3, 或在 i 的阶为 2, 证毕.

设 $L = \mathbb{Z}+\mathbb{Z}\tau$, $M = \mathbb{Z}+\mathbb{Z}_{\tau'}$ 为两个格, $\tau, \tau' \in \mathfrak{H}$, 若 $j(L) = j(\tau) = j(\tau') = j(M)$, 由定理 2.4, 存在 $\alpha \in \Gamma$, 使得 $\tau' = \alpha(\tau)$, 即 $L = M$.

推论 2.1 *设 L 和 M 为两个格, 当且仅当 $L = M$ 时 $j(L) = j(M)$.*

$g_2(\tau)$ 和 $g_3(\tau)$ 都是 $\mathfrak{H}$ 上的全纯函数, 在 ∞ 的阶都为零, 由命题 2.3 可得

$$\frac{1}{3}\mathrm{ord}_\rho(g_2) + \frac{1}{2}\mathrm{ord}_i(g_2) + \sum_{P \neq i,\rho} \mathrm{ord}_P(g_2) = \frac{1}{3}$$

及

$$\frac{1}{3}\mathrm{ord}_\rho(g_3) + \frac{1}{2}\mathrm{ord}_i(g_3) + \sum_{P \neq i,\rho} \mathrm{ord}_P(g_3) = \frac{1}{2}.$$

对任一 $P \neq i, \rho$, $\mathrm{ord}_P(g_2)$ 和 $\mathrm{ord}_P(g_3)$ 都是非负整数, 所以 $g_2(\tau)$ 仅在 $\tau = \rho$ 有零点, 阶为 1; $g_3(\tau)$ 仅在 $\tau = i$ 有零点, 阶也为 1. 由定理 2.4 的证明可知, $j(\tau)$ 仅在 $\tau = \rho$ 有零点, 阶为 3.

定理 2.5　设 c_2 和 c_3 为复数, 且

$$c_2^3 - 27c_3^2 \neq 0,$$

则存在一个格 L, 使得 $c_2 = g_2(L)$, $c_3 = g_3(L)$, 因而椭圆曲线

$$y^2 = 4x^3 - c_2x - c_3$$

与 $\mathbb{C}/L$ 同构.

证明　由定理 2.4, 存在 $\tau \in \mathfrak{H}$, 使得

$$j(\tau) = 1728 \cdot \frac{c_2^3}{c_2^3 - 27c_3^2}.$$

记 $M = \mathbb{Z} + \mathbb{Z}\tau$, 若 $c_2 = 0$, 则 $j(\tau) = 0$, $\tau = \rho$. 存在 $\omega \in \mathbb{C}^*$(非零复数集合), 使得 $\omega^{-6}g_3(M) = c_3$. 令 $L = \omega M$, 则

$$\begin{aligned} g_2(L) &= g_2(\omega M) = \omega^{-6}g_2(\rho) = c_2 = 0, \\ g_3(L) &= g_3(\omega M) = \omega^{-6}g_3(M) = c_3. \end{aligned}$$

若 $c_2 \neq 0$, 取 $\omega \in \mathbb{C}^*$, 使得 $\omega^{-4}g_2(M) = c_2$. 令 $L = \omega M$, 则 $g_2(L) = c_2$. 由

$$\begin{aligned} 1728 \cdot \frac{c_2^3}{c_2^3 - 27c_3^2} &= j(\tau) = j(M) = j(L) \\ &= 1728 \cdot \frac{g_2^3(L)}{g_2^3(L) - 27g_3^2(L)} \\ &= 1728 \cdot \frac{c_2^3}{c_2^3 - 27g_3^2(L)}, \end{aligned}$$

可见 $g_3^2(L) = c_3^2$, $g_3(L) = \pm c_3$, 必要时, 以 $i\omega$ 代替 ω, 这不改变 $g_2(L)$, 而将 $g_3(L)$ 改变符号. 因而使得 $g_2(L) = c_2$, $g_3(L) = c_3$, 证毕.

§2.3　同种椭圆曲线

设椭圆曲线 E 到椭圆曲线 $\widetilde{E}$ 有一个有理变换

$$\begin{aligned} \varphi:\ & E \longrightarrow \widetilde{E} \\ & (x, y) \longmapsto (X, Y) \\ & \mathcal{O} \longmapsto \mathcal{O} \end{aligned}$$

(即 X, Y 是 x, y 的有理函数), φ 将 $\mathcal{O}$ 映为 $\mathcal{O}$ 且是一个群同态, 则 φ 称为同种映射, $\widetilde{E}$ 称为 φ 的同种曲线 (实际上, 有理变换 φ 若将 $\mathcal{O}$ 映为 $\mathcal{O}$, 则可以证明 φ 一定是群同态. 证明见文献 [12]).

设定义 E 的方程为

$$y^2 = 4x^3 - g_2x - g_3, \tag{2.10}$$

定义 $\widetilde{E}$ 的方程为

$$Y^2 = 4X^3 - \widetilde{g_2}X - \widetilde{g_3}.$$

由定理 2.5, 存在格 L 和 M, 使得 $E \simeq \mathbb{C}/L$, $\widetilde{E} \simeq \mathbb{C}/M$, 同时存在复数 $c \neq 0$, 使得同种 φ 诱导 $\mathbb{C}/L$ 到 $\mathbb{C}/M$ 的映射为

$$\begin{aligned} \lambda: \quad \mathbb{C}/L &\longrightarrow \mathbb{C}/M \\ z \quad &\longmapsto cz \end{aligned}$$

由命题 2.1 即知下列图可交换:

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\lambda} & \mathbb{C}/M \\ \downarrow & & \downarrow \\ E & \xrightarrow[\varphi]{} & \widetilde{E} \end{array}$$

易见 $cL \subset M$, 从而 $L \subset c^{-1}M$. $F = c^{-1}M/L$ 是映射 λ 的核, 它是 $\mathbb{C}/L$ 中的一个有限子群. F 与 E 上一个子群同构, 仍记为 F, 它也是同种 φ 的核, 所以从群同构来说, $\widetilde{E} = E/F$. 我们将 $|F|$ 称为同种变换 φ 的阶.

命题 2.4 给定 $\mathbb{C}/L \simeq E$ 上任一有限子群 F, 可以构造 E 的同种椭圆曲线 $\widetilde{E}$, 使得 $\widetilde{E} \simeq E/F$(有时用 E/F 代表 $\widetilde{E}$).

证明 令 $L = \mathbb{Z} + \mathbb{Z}\tau$,

$$F = \{x_i + y_i\tau \,|\, 0 \leqslant x_i,\, y_i < 1,\, 1 \leqslant i \leqslant m\}.$$

定义格

$$M = \{x_i + y_i\tau + L \,|\, 0 \leqslant x_i,\, y_i < 1,\, 1 \leqslant i \leqslant m\},$$

则 $L \subset M$. 构造椭圆曲线 $\widetilde{E} \simeq \mathbb{C}/M$, 则映射

$$\begin{aligned} \mathbb{C}/L &\longrightarrow \mathbb{C}/M \\ z \quad &\longmapsto z \end{aligned}$$

诱导同种映射

$$\varphi: \quad E \longrightarrow \widetilde{E},$$

φ 的核为 $M/L \simeq F$, 故 $\widetilde{E} \simeq E/F$, 证毕.

下述定理 2.6 将给出同种映射 φ 的表达式, 仍设 F 为 E 的子群, 以下仅需考虑 F 为奇数阶子群. 令 $F - \{\mathcal{O}\} = R \cup (-R)$, $R \cap (-R) = \varnothing$. 曲线 E 由 (2.10) 式定义, 以 $\theta = \big(x(\theta), y(\theta)\big) = (x_\theta, y_\theta)$ 记 E 上的点, 定义 $t_\theta = 12x_\theta^2 - g_2$.

定理 2.6[13](Vélu 定理)　设同种映射

$$\begin{aligned}\varphi:\ E &\longrightarrow \widetilde{E} = E/F\\ (x, y) &\longmapsto (X, Y),\end{aligned}$$

则

$$\begin{aligned}X &= x + \sum_{\theta \in R}\left(\frac{t_\theta}{2(x - x_\theta)} + \frac{y_\theta^2}{(x - x_\theta)^2}\right),\\ Y &= y - \sum_{\theta \in R}\left(\frac{y t_\theta}{2(x - x_\theta)^2} + \frac{2y y_\theta^2}{(x - x_\theta)^3}\right) = y\frac{dX}{dx}.\end{aligned} \tag{2.11}$$

令

$$t = \sum_{\theta \in R} t_\theta, \quad \omega = \sum_{\theta \in R}\big(8y_\theta^2 + 4t_\theta x_\theta\big),$$

则定义 $\widetilde{E}$ 的方程为

$$Y^2 = 4X^3 - \widetilde{g_2}X - \widetilde{g_3},$$

其中

$$\widetilde{g_2} = g_2 + 10t, \quad \widetilde{g_3} = (g_3 + 14\omega)/4.$$

证明　记 $P = (x, y)$ 为 E 上的点, 定义

$$\begin{aligned}X(P) &= x + \sum_{\theta \in F - \{\mathcal{O}\}}\big[x(P + \theta) - x(\theta)\big],\\ Y(P) &= y + \sum_{\theta \in F - \{\mathcal{O}\}}\big[y(P + \theta) - y(\theta)\big],\end{aligned}$$

X 和 Y 是定义在 E/F 上的函数, 利用 §2.1 中所给出的 E 上的加法运算规则,

$$\begin{aligned}&x(P + \theta) - x(\theta) + x(P - \theta) - x(-\theta)\\ =& -2x - 4x_\theta + \frac{1}{4(x - x_\theta)^2}\big((y - y_\theta)^2 + (y + y_\theta)^2\big)\\ =& \frac{1}{2(x - x_\theta)^2}\big(y^2 + y_\theta^2 - 4(x + 2x_\theta)(x - x_\theta)^2\big)\\ =& \frac{1}{2(x - x_\theta)^2}\big(x(12x_\theta^2 - g_2) - 4x_\theta^3 - g_2 x_\theta - 2g_3\big)\\ =& \frac{t_\theta}{2(x - x_\theta)} + \frac{y_\theta^2}{(x - x_\theta)^2},\end{aligned}$$

$$
\begin{aligned}
& y(P+\theta)-y(\theta)+y(P-\theta)-y(-\theta) \\
= & \left(\frac{y-y_\theta}{x-x_\theta}\right)(x-x(P+\theta))+\left(\frac{y+y_\theta}{x-x_\theta}\right)(x-x(P-\theta))-2y \\
= & \left(\frac{y-y_\theta}{x-x_\theta}\right)\left(2x+x_\theta-\frac{1}{4}\left(\frac{y-y_\theta}{x-x_\theta}\right)^2\right) \\
& +\left(\frac{y+y_\theta}{x-x_\theta}\right)\left(2x+x_\theta-\frac{1}{4}\left(\frac{y+y_\theta}{x-x_\theta}\right)^2\right)-2y \\
= & \frac{2y(x+2x_\theta)}{x-x_\theta}-\frac{2y^3+6yy_\theta^2}{4(x-x_\theta)^3} \\
= & \frac{y}{2(x-x_\theta)^3}(4(x+2x_\theta)(x-x_\theta)^2-y^2-3y_\theta^2) \\
= & \frac{y}{2(x-x_\theta)^3}(-x(12x_\theta^2-g_2)-4x_\theta^3+3g_2x_\theta+4g_3) \\
= & -\frac{yt_\theta}{2(x-x_\theta)^2}-\frac{2yy_\theta^2}{(x-x_\theta)^3}.
\end{aligned}
$$

由此得到 (2.11) 式.

由于 $\mathrm{ord}_{\mathcal{O}}(x)=-2$, $\mathrm{ord}_{\mathcal{O}}(y)=-3$, 令 $z=-x/y$, 故 $\mathrm{ord}_{\mathcal{O}}(z)=1$, x 和 y 在 $\mathcal{O}$ 附近可以展开为 z 的幂级数. 设

$$
x=\sum_{i=-2}^{\infty}\alpha_i z^i,
$$

则

$$
y=-\sum_{i=-2}^{\infty}\alpha_i z^{i-1},
$$

由关系式 $y^2=4x^3-g_2x-g_3$ 可得到系数 α_i.

$$
\begin{aligned}
x &= \frac{1}{4}z^{-2}+g_2z^2+g_3z^4+\cdots, \\
y &= -\frac{1}{4}z^{-3}-g_2z+g_3z^3-\cdots,
\end{aligned}
$$

利用 (2.11) 式, 我们有

$$
\begin{aligned}
X &= x+\sum\left[\frac{t_\theta}{2}\left(\frac{1}{x}+\frac{x_\theta}{x^2}+\cdots\right)+y_\theta^2\left(\frac{1}{x^2}+\cdots\right)\right] \\
&= \frac{1}{4}z^{-2}+(g_2+2t)z^2+(g_3+2\omega)z^4+\cdots, \\
Y &= y-y\sum\left[2y_\theta^2\left(\frac{1}{x^3}+\cdots\right)+\frac{t_\theta}{2}\left(\frac{1}{x^2}+\frac{2x_\theta}{x^3}+\cdots\right)\right] \\
&= -\frac{1}{4}z^{-3}-(g_2-2t)z-(g_3-4\omega)z^3+\cdots.
\end{aligned}
$$

将 X 和 Y 的展开式代入 $Y^2 = 4X^3 - \widetilde{g_2}X - \widetilde{g_3}$, 得到

$$\widetilde{g_2} = g_2 + 10t,\ \widetilde{g_3} = (g_3 + 14\omega)/4.$$

证毕.

令

$$H(x) = \prod_{\theta \in R} (x - x_\theta).$$

推论 2.2　同种映射 φ: $E \to \widetilde{E} = E/F$ 可表为

$$\varphi(x,y) = \left(\frac{G(x)}{2H(x)^2}, \frac{J(x,y)}{2H(x)^3}\right),$$

其中 $H(x)$ 次数为 $|R|$, $G(x)$ 的次数为 $|F|$, H, G, J 的系数都是 x_θ, y_θ, g_2, g_3 的整系数多项式.

§2.4　除子多项式

设 E 为方程 (2.1) 的椭圆曲线, $E \simeq \mathbb{C}/L$, $L = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$, $\omega_1/\omega_2 \in \mathfrak{H}$, 设 $n \geqslant 1$ 为正整数, 令

$$\begin{aligned}(\mathbb{C}/L)_n &= \{u \in \mathbb{C}/L \mid nu \in L\} \\ &= \left\{\frac{s}{n}\omega_1 + \frac{t}{n}\omega_2 \,\middle|\, 0 \leqslant s,\ t < n,\ s,t \text{ 为整数}\right\},\end{aligned}$$

$(\mathbb{C}/L)_n$ 对应 E 上的点集

$$\begin{aligned}E[n] &= \{p \in E \mid nP = \mathcal{O}\} \\ &= \left\{\left(\wp\left(\frac{s}{n}\omega_1 + \frac{t}{n}\omega_2\right), \wp'\left(\frac{s}{n}\omega_1 + \frac{t}{n}\omega_2\right)\right) \,\middle|\, 0 \leqslant s,\ t \leqslant n,\right. \\ &\qquad \left. s,t \in \mathbb{Z},\ s,t \text{ 不同时为零}\right\} \bigcup \{\mathcal{O}\},\end{aligned}$$

$E[n]$ 中的点称为 E 的 n 阶挠点. 本节研究多项式

$$\prod_{\substack{u \not\equiv 0 \pmod L \\ nu \equiv 0 \pmod L}} (x - \wp(u)),$$

我们将证明该多项式的系数在 $\mathbb{Z}[a,b]$ 之中, 其中 $a = -g_2/4$, $b = -g_3/4$, 并给出计算这些多项式的递推关系式. 换句话说, 我们要找出以 $E[n]$ 中所有非 $\mathcal{O}$ 点的 x 坐标为根的多项式, 该多项式称为除子多项式.

定义椭圆函数 $f_n(z)$, 使得

$$f_n(z)^2 = n^2 \prod_{\substack{u \not\equiv 0 \pmod L \\ nu \equiv 0 \pmod L}} (\wp(z) - \wp(u)). \tag{2.12}$$

今证右端的乘积是一个完全平方. 当 $u \not\equiv 0 \pmod L$, $nu \equiv 0 \pmod L$ 时, 若 $u \not\equiv -u \pmod L$, 则 $\wp(z) - \wp(u)$ 在乘积中出现 2 次. 若 $u \equiv -u \pmod L$(这时 n 一定是偶数), 则 u 必定为 $\omega_1/2, \omega_2/2, (\omega_1+\omega_2)/2$ 之一, 而

$$\left(\wp(z) - \wp\left(\frac{\omega_1}{2}\right)\right)\left(\wp(z) - \wp\left(\frac{\omega_2}{2}\right)\right)\left(\wp(z) - \wp\left(\frac{\omega_1+\omega_2}{2}\right)\right) = \frac{1}{4}\left(\wp'(z)\right)^2,$$

所以上述乘积为完全平方. 由此可知当 n 为奇数时,

$$f_n = P_n(\wp) = n\wp^{(n^2-1)/2} + \cdots,$$

当 n 为偶数时,

$$f_n = \frac{1}{2}\wp'\widetilde{P_n}(\wp) = \frac{n}{2}\wp'\left(\wp^{(n^2-4)/2} + \cdots\right).$$

P_n 和 $\widetilde{P_n}$ 都是 $\wp$ 的多项式, f_n 在 $z=0$ 的展开式为

$$f_n = \frac{(-1)^{n-1}n}{z^{n^2-1}} + \cdots,$$

$f_n(z)$ 以 $(\mathbb{C}/L)_n$ 中的非零点为 1 阶零点, 以 $z=0$ 为 n^2-1 阶极点.

定理 2.7 设 $n \geqslant 2$ 为整数, 则 (令 $f_1(z)=1$)

$$\wp(nz) = \wp(z) - \frac{f_{n+1}(z)f_{n-1}(z)}{f_n^2(z)}, \quad \wp'(nz) = \frac{f_{2n}(z)}{f_n^4(z)}.$$

证明 易见 $g(z) = \wp(nz) - \wp(z)$ 以 $(\mathbb{C}/L)_n$ 中每个点为 2 阶极点, 它在 $\mathbb{C}/L$ 上共有 $2n^2$ 个极点. 当 $u \in (\mathbb{C}/L)_{n\pm1}$ 时, $nu \equiv \pm u \pmod L$, 故 $g(z)$ 以 $(\mathbb{C}/L)_{n\pm1}$ 中的非零点为它的零点 (注意: $(n+1)^2-1+(n-1)^2-1=2n^2$). 当 n 为偶数时, $(n+1,n-1)=1$, 故 $(\mathbb{C}/L)_{n+1} \cap (\mathbb{C}/L)_{n-1} = \{0\}$, $(\mathbb{C}/L)_{n\pm1}$ 中每个非零点都是 $g(z)$ 的 1 阶零点. 当 n 为奇数时, $(n+1,n-1)=2$, 故 $(\mathbb{C}/L)_{n+1} \cap (\mathbb{C}/L)_{n-1} = (\mathbb{C}/L)_2$. 由于 $g'(z) = n\wp'(nz) - \wp'(z)$, 可见 $(\mathbb{C}/L)_2$ 中的非零点为 $g(z)$ 的 2 阶零点, 而 $(\mathbb{C}/L)_{n\pm1}$ 中其余非零点为 $g(z)$ 的 1 阶零点, 因而椭圆函数 $\frac{f_n^2(z)(\wp(nz)-\wp(z))}{f_{n+1}(z)f_{n-1}(z)}$ 既没有极点, 也没有零点, 是一个常数 (Liouville 定理). 它在 $z=0$ 的值为 $\frac{n^2(\frac{1}{n^2}-1)}{(n+1)(n-1)} = -1$, 从而定理中第一个等式得证.

$\wp'(nz)$ 在 $(\mathbb{C}/L)_n$ 中每个点有 3 阶极点, 它在 $\mathbb{C}/L$ 上共有 $3n^2$ 个极点. $\wp'(z)$ 以 $(\mathbb{C}/L)_2$ 中的非零点为 1 阶零点, 故 $\wp'(nz)$ 以 $(\mathbb{C}/L)_{2n} \setminus (\mathbb{C}/L)_n$ 中各点为 1 阶零点, 这批零点共有 $(2n)^2 - 1 - (n^2 - 1) = 3n^2$ 个, 所以 $\frac{f_n^4(z)\wp'(nz)}{f_{2n}(z)}$ 既没有极点也没有零点, 是一个常数, 它在 $z = 0$ 的值为 $\frac{n^4(\frac{-2}{n^3})}{2n} = 1$, 证得第 2 个等式. 定理 2.7 证毕.

令 $f_1(z) = 1$, 我们有 $f_2(z) = \wp'(z)$. 今计算 $f_3(z)$ 和 $f_4(z)$.

首先, 由 E 上的加法运算公式可得

$$\begin{aligned}\wp(2z) &= \frac{1}{4}\left(\frac{12\wp^2(z) - g_2}{2\wp'(z)}\right)^2 - 2\wp(z)\\ &= \frac{\wp^4(z) + 2^{-1}g_2\wp^2(z) + 2g_3\wp(z) + \frac{g_2^2}{16}}{\wp'(z)^2},\end{aligned} \tag{2.13}$$

$$\begin{aligned}\wp'(2z) &= \left(\frac{12\wp^2(z) - g_2}{2\wp'(z)}\right)\left(\wp(z) - \frac{\wp^4(z) + 2^{-1}g_2\wp^2(z) + 2g_3\wp(z) + \frac{g_2^2}{16}}{\wp'(z)^2}\right) - \wp'(z)\\ &= \frac{1}{2\wp'(z)^3}\left(4\wp(z)^6 - 5g_2\wp(z)^4 - 20g_3\wp(z)^3 - \frac{5g_2^2\wp(z)^2}{4} - g_2g_3\wp(z) + \frac{g_2^3}{16} - 2g_3^2\right),\end{aligned} \tag{2.14}$$

由定理 2.7 的第 1 式及 (2.13) 式得

$$\begin{aligned}f_3(z) &= f_2(z)^2\big(\wp(z) - \wp(2z)\big)\\ &= 3\wp(z)^4 - \frac{3g_2\wp(z)^2}{2} - 3g_3\wp(z) - \frac{g_2^2}{16},\end{aligned}$$

由定理 2.7 的第 2 式及 (2.14) 式得

$$\begin{aligned}f_4(z) = f_2(z)^4\wp'(2z) = \frac{1}{2}\wp'(z)\Big(&4\wp(z)^6 - 5g_2\wp(z)^4\\ &- 20g_3\wp(z)^3 - \frac{5g_2^2\wp(z)^2}{4} - g_2g_3\wp(z) + \frac{g_2^3}{16} - 2g_3^2\Big).\end{aligned}$$

当 $n \geqslant 5$ 时, 可利用下述递推公式计算 $f_n(z)$.

定理 2.8 设 $m > n \geqslant 1$, 则

$$f_{m+1}f_{m-1}f_n^2 - f_{n+1}f_{n-1}f_m^2 = f_{m+n}f_{m-n}.$$

证明 由定理 2.7 可得

$$\wp(mz)-\wp(nz)=\frac{1}{f_m^2f_n^2}\Big(f_{n+1}f_{n-1}f_m^2-f_{m+1}f_{m-1}f_n^2\Big).$$

以 $g(z)$ 表示上式左端的函数, 设 $d=(m,n)$, 则

$$(\mathbb{C}/L)_m\bigcap(\mathbb{C}/L)_n=(\mathbb{C}/L)_d.$$

$g(z)$ 在 $(\mathbb{C}/L)_m\setminus(\mathbb{C}/L)_d$, $(\mathbb{C}/L)_n\setminus(\mathbb{C}/L)_d$ 和 $(\mathbb{C}/L)_d$ 中各点有 2 阶极点, 它在 $\mathbb{C}/L$ 上共有 $2(m^2+n^2-d^2)$ 个极点.

若 u 适合 $mu\equiv\pm nu\not\equiv 0 \pmod L$, 则 u 是 $g(z)$ 的零点, 故 $(\mathbb{C}/L)_{m+n}\setminus(\mathbb{C}/L)_d$ 和 $(\mathbb{C}/L)_{m-n}\setminus(\mathbb{C}/L)_d$ 都是 $g(z)$ 的零点, 这两个集合的点数之和为 $(m+n)^2-d^2+(m-n)^2-d^2=2(m^2+n^2-d^2)$, 与 $g(z)$ 在 $\mathbb{C}/L$ 中的极点个数相同. 为了证明这两个集合已是 $g(z)$ 在 $\mathbb{C}/L$ 中的全部集合, 仅需证明它们的公共点都是 $g(z)$ 的 2 阶零点. 记 $s=(m+n,m-n)$, 我们有

$$\begin{aligned}((\mathbb{C}/L)_{m+n}\setminus(\mathbb{C}/L)_d)&\bigcap((\mathbb{C}/L)_{m-n}\setminus(\mathbb{C}/L)_d)\\&=((\mathbb{C}/L)_{m+n}\bigcap(\mathbb{C}/L)_{m-n})\setminus(\mathbb{C}/L)_d\\&=(\mathbb{C}/L)_s\setminus(\mathbb{C}/L)_d.\end{aligned}\tag{2.15}$$

设 u 适合 $mu\equiv\pm nu\not\equiv 0 \pmod L$, 这时

$$g'(u)=m\wp'(mu)-n\wp'(nu)=(m\pm n)\wp'(mu),$$

可见 $g(z)$ 的 2 阶零点为 $\big((\mathbb{C}/L)_{m\pm n}\cap(\mathbb{C}/L)_{2m}\big)\setminus\big(\mathbb{C}/L\big)_d$, 易见 $(m\pm n,2m)=(m+n,m-n)=s$, 故

$$((\mathbb{C}/L)_{m\pm n}\bigcap(\mathbb{C}/L)_{2m})\setminus(\mathbb{C}/L)_d=(\mathbb{C}/L)_s\setminus(\mathbb{C}/L)_d,$$

与 (2.15) 式右端相同. 综合上述, 可见

$$\frac{f_n^2f_m^2\big(\wp(mz)-\wp(nz)\big)}{f_{m+n}f_{m-n}}=\frac{f_{n+1}f_{n-1}f_m^2-f_{m-1}f_{m+1}f_n^2}{f_{m+n}f_{m-n}}$$

为常数, 它在 $z=0$ 的值为

$$\frac{(n+1)(n-1)m^2-(m-1)(m+1)n^2}{(m+n)(m-n)}=-1.$$

证毕.

在定理 2.8 中特别取 $(m,n)=(n+1,n)$ 和 $(m,n)=(n+1,n-1)$ 得

定理 2.9 我们有

$$f_{2n+1} = f_{n+2}f_n^3 - f_{n+1}^3 f_{n-1}, \qquad n \geqslant 2,$$
$$f_2 f_{2n} = f_n\big(f_{n+2}f_{n-1}^2 - f_{n+1}^2 f_{n-2}\big), \qquad n > 2.$$

为了使 f_n 的系数都变为整数, 取

$$x = \wp(z), \quad y = \frac{1}{2}\wp'(z), \quad a = -\frac{1}{4}g_2, \quad b = -\frac{1}{4}g_3,$$

这时 x, y 适合方程

$$E': \quad Y^2 = X^3 + aX + b. \tag{2.16}$$

令 $\psi_n(x,y) = f_n(\wp, \wp')$, 有

$$\begin{aligned}
\psi_1 &= 1,\\
\psi_2 &= 2y,\\
\psi_3 &= 3x^4 + 6ax^2 + 12bx - a^2,\\
\psi_4 &= 4y(x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2),\\
\psi_{2n+1} &= \psi_{n+2}\psi_n^3 - \psi_{n-1}\psi_{n+1}^3, \qquad n \geqslant 2,\\
\psi_{2n} &= \psi_n(\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2)/2y, \quad n > 2.
\end{aligned}$$

用归纳法可以证明, ψ_{2n} 能被 $2y$ 整除.

由 (2.12) 式可得

定理 2.10 设 $P = (x,y)$ 为 $E' \setminus \{\mathcal{O}\}$ 上一点, $n \geqslant 2$, 则 $P \in E'[n]$ 当且仅当 $\psi_n(P) = 0$.

由定理 2.7 可得

定理 2.11 设 $P = (x,y) \in E' \setminus E'[n]$, $n \geqslant 2$, 则

$$nP = \left(x - \frac{\psi_{n-1}\psi_{n+1}}{\psi_n^2}, \frac{\psi_{n+2}\psi_{n-1}^2 - \psi_{n-2}\psi_{n+1}^2}{4y\psi_n^3}\right).$$

由于 $P \mapsto nP$ 是 E' 上的一个同种映射, 定理 2.11 是推论 2.2 的一个特例. 令

$$f_n(x) = \begin{cases} \psi_n, & n \text{ 为奇数},\\ \psi_n/\psi_2, & n \text{ 为偶数}. \end{cases}$$

当 n 为奇数时, f_n 的次数为 $(n^2-1)/2$, 当 n 为偶数时, f_n 的次数为 $(n^2-4)/2$, 由定理 2.9 可得

推论 2.3 设 $P = (x,y) \in E' \setminus \{\mathcal{O}\}$, 且 $2P \neq \mathcal{O}$, $n \geqslant 2$, 则 $P \in E'[n]$ 当且仅当 $f_n(x) = 0$.

§2.5 模多项式

设 n 为正整数, 定义 2 阶整数矩阵集合

$$\Delta_n^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbb{Z},\ ad - bc = n,\ (a, b, c, d) = 1 \right\}.$$

令 $\Gamma = \mathrm{SL}_2(\mathbb{Z})$.

引理 2.1 $\Delta_n^* = \Gamma \cdot \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix} \cdot \Gamma$.

证明 由初等因子定理, Δ_n^* 中任一矩阵可通过行和列的初等变换变为对角形

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

且 $a|d$. 又由于 $(a, d) = 1$, 故 $a = 1$, $d = n$, 证毕.

Δ_n^* 中任一矩阵可通过行的初等变换变为

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \tag{2.17}$$

其中 $a > 0$, $d > b \geqslant 0$, $ad = n$, 即 Δ_n^* 中任一矩阵与形如 (2.17) 式的某一矩阵属于 Γ 的同一左陪集. 若形如 (2.17) 式的两个矩阵

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}, \qquad \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix} \tag{2.18}$$

属于 Γ 的同一左陪集, 即存在 $\begin{pmatrix} g & h \\ e & f \end{pmatrix} \in \Gamma$, 使得

$$\begin{pmatrix} g & h \\ e & f \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}.$$

由 $ea = 0$, 得 $e = 0$, 从而 $g = f = \pm 1$, 但 $ga = a'$, 故 $g = f = 1$, 再由 $b + hd = b'$, 可知 $h = 0$, 所以 (2.18) 式中两个矩阵相同. 记 (2.17) 式的矩阵个数为 $\psi(n)$, 即 Δ_n^* 是 $\psi(n)$ 个 Γ 的左陪集之并. 今计算 $\psi(n)$.

由于 $ad = n$, 当 d 确定时, a 随之确定. 记 $e = (a, d)$, 这时 b 一定与 e 互素, 故 b 可能的个数为 $\frac{d}{e}\varphi(e)$ (φ 为欧拉函数), 因而 $\psi(n) = \sum_{d|n} \frac{d}{e}\varphi(e)$.

$\psi(n)$ 是积性函数, 即若 $n = n_1 n_2$, $(n_1, n_2) = 1$, 则 $\psi(n) = \psi(n_1)\psi(n_2)$. 事实上, 若 $a = a_1 a_2$, $d = d_1 d_2$, $a_i | n_i$, $d_i | n_i$, 则 $e = e_1 e_2$, $e_i = (a_i, d_i)$,

$$\psi(n_1 n_2) = \sum_{\substack{d_1 | n_1 \\ d_2 | n_2}} \frac{d_1 d_2}{e_1 e_2} \varphi(e_1)\varphi(e_2) = \psi(n_1)\psi(n_2).$$

所以仅需计算 $\psi(p^r)$, p 为素数. 我们有

$$\begin{aligned}\psi(p^r) &= 1 + p^r + \sum_{v=1}^{r-1} \frac{p^v}{e} \cdot e\left(1 - \frac{1}{p}\right) \\ &= 1 + p^r + \sum_{v=1}^{r-1} (p^v - p^{v-1}) \\ &= p^r\left(1 + \frac{1}{p}\right),\end{aligned}$$

故

$$\psi(n) = n \prod_{p|n} \left(1 + \frac{1}{p}\right),$$

这里 p 跑遍 n 的素因子. 特别当 $n = p$ 为素数时, $\psi(p) = p + 1$.

以

$$\{\alpha_i\}, \quad i = 1, 2, \cdots, \psi(n)$$

表示 (2.17) 式中矩阵, 因而

$$\Delta_n^* = \bigcup_{i=1}^{\psi(n)} \Gamma\alpha_i.$$

设 $\gamma \in \Gamma$, 由引理 2.1

$$\Delta_n^* = \Delta_n^* \cdot \gamma = \bigcup_{i=1}^{\psi(n)} \Gamma\alpha_i\gamma = \bigcup_{i=1}^{\psi(n)} \Gamma\alpha_i, \tag{2.19}$$

即 $\{\Gamma\alpha_i\gamma \,|\, i = 1, 2, \cdots, \psi(n)\}$ 是 $\{\Gamma\alpha_i \,|\, i = 1, 2, \cdots, \psi(n)\}$ 的一个置换.

引理 2.2　*设 $f(\tau)$ 为 Γ 上的模函数, 在 $\mathfrak{H}$ 上全纯, 具有 q 展开式*

$$f = \sum_{n=-M}^{\infty} c_n q^n,$$

则 f 是 j 的多项式, 其系数在 $\mathbb{Z}[c_{-M}, c_{-M+1}, \cdots, c_0]$ 之中.

证明　由于

$$f = \frac{c_{-M}}{q^M} + \text{高次项},$$

所以 $f - c_{-M}j^M$ 是 $\mathfrak{H}$ 上全纯模函数, 它的 q 展开式中最低幂次为 $-M+1$. 这里利用了 j 的 q 展开式 (2.8). 重复上述过程, 直到得到一个在 $\mathfrak{H}$ 上全纯、q 展开式中仅含正幂次项的模函数, 它一定恒为零 (命题 2.3), 证毕.

设 $\gamma \in \Gamma$, γ 在函数 $f(\tau)$ 上的作用记为 $f \circ \gamma = f\big(\gamma(\tau)\big)$. j 是 Γ 上的模函数, 故对任一 $\gamma \in \Gamma$, 有 $j \circ \gamma = j$.

定义

$$\Phi_n(X) = \prod_{i=1}^{\psi(n)} (X - j \circ \alpha_i), \tag{2.20}$$

$\Phi_n(X)$ 的系数为 $j \circ \alpha_i$ 的初等对称多项式, 为 $\mathfrak{H}$ 上的全纯函数, 由 (2.19) 式, 任取 $\gamma \in \Gamma$, 对任一 α_i, 存在惟一的 α_j 及 $\gamma' \in \Gamma$, 使得 $\alpha_i\gamma = \gamma'\alpha_j$, 因而

$$j \circ \alpha_i\gamma = j \circ \gamma'\alpha_j = j \circ \alpha_j,$$

所以 $\Phi_n(X)$ 的系数在 Γ 作用下不变, 而且在 ∞ 是亚纯的, 这些系数都是 Γ 上的椭圆函数. 记 (2.8) 式为

$$j = q^{-1} + P(q),$$

其中 P 为 q 的整系数幂级数. 设

$$\alpha_i = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

则

$$j \circ \alpha_i = \frac{1}{q^{a/d} \cdot \zeta_d^b} + P\big(q^{a/d} \cdot \zeta_d^b\big), \tag{2.21}$$

其中 $\zeta_d = e^{2\pi i/d}$ 是 d 次单位根. 可见在 $\Phi_n(X)$ 的系数所对应的 q 展开式中, 其系数都属于分圆域 $\mathbb{Q}(\zeta_n)$ $(\zeta_n = e^{2\pi i/n})$. 考虑 $\mathbb{Q}(\zeta_n)$ 的任一同构 σ_r:

$$\sigma_r: \quad \zeta_n \longrightarrow \zeta_n^r,$$

这里 r 与 n 互素, 将它作用到 $\Phi_n(X)$ 的系数所对应的 q 展开式的系数上, 由 (2.21) 式可见它产生 $j \circ \alpha_i$ 的一个置换, 所以 $\Phi_n(X)$ 的系数在 σ_r 的作用下不变, 它们对应的 q 展开式具有整系数. 利用引理 2.2, 可见 $\Phi_n(X)$ 的系数都是 j 的整数多项式, 即

$$\Phi_n(X) = \Phi_n(X, j) \in \mathbb{Z}[X, j].$$

称 $\Phi_n(X)$ 为 n 阶模多项式, 它是 X 的 $\psi(n)$ 次多项式.

设 $M=\mathbb{Z}\tau_1+\mathbb{Z}\tau_2$, $L=\mathbb{Z}\omega_1+\mathbb{Z}\omega_2$ 为两个格, $\tau=\tau_1/\tau_2\in\mathfrak{H}$, $\omega=\omega_1/\omega_2\in\mathfrak{H}$, 且 $M\subset L$, $[L:M]=n$, 则有

$$\tau_1=a\omega_1+b\omega_2,\quad \tau_2=c\omega_1+d\omega_2,$$

且 $ad-bc=n$, 易见

$$\omega_1=\frac{1}{n}(d\tau_1-c\tau_2),\quad \omega_2=\frac{1}{n}(-b\tau_1+a\tau_2),$$

由初等因子定理, 存在 $\gamma_1,\gamma_2\in\Gamma$, 使得

$$\gamma_1\begin{pmatrix} a & b\\ c & d\end{pmatrix}\gamma_2=\begin{pmatrix} p & 0\\ 0 & q\end{pmatrix},\qquad p|q,\ pq=n,$$

这时 $L/M\simeq G_1\oplus G_2$, G_1 和 G_2 分别为 p 阶和 q 阶循环群. 当且仅当 $p=1$ 时, L/M 为 n 阶循环群, 换句话说, 当且仅当 $\alpha=\left(\begin{smallmatrix} a & b\\ c & d\end{smallmatrix}\right)\in\Delta_n^*$ 时, L/M 为 n 阶循环群, 我们有 $j(M)=j(\tau)$, $j(L)=j(\omega)=j\left(\frac{d\tau-c}{-b\tau+a}\right)=j\left(n\alpha^{-1}(\tau)\right)$, 易见 $n\alpha^{-1}\in\Delta_n^*$. 于是由 (2.20) 式得到:

定理 2.12　设 φ: $E_1\to E_2$ 为 n 阶同种变换. 当且仅当 φ 的核为 n 阶循环子群时, $j(E_2)$ 是 $\Phi_n\left(x,j(E_1)\right)$ 的根.

定理 2.13　(i) $\Phi_n(X,j)$ 是 $\mathbb{C}(j)$ 上次数为 $\psi(n)$ 的不可约多项式;

(ii) $\Phi_n(X,j)=\Phi_n(j,X)$;

(iii) 若 n 不是完全平方, 则 $\Phi_n(j,j)$ 是次数大于 1 的关于 j 的多项式, 且首项系数为 ±1.

证明　显然 Φ_n 关于 X 的次数为 $\psi(n)$. 于是第一断言可由以下事实推出: Γ 可迁地置换函数 $j\circ\alpha_i$ $(1\leqslant i\leqslant\psi(n))$, 且作用在域 $\mathbb{C}(j,j\circ\alpha_1,\cdots,j\circ\alpha_{\psi(n)})$ 上作为一个自同构群. 因此, 若 $\Phi_n(X)$ 在 $\mathbb{C}(j)$ 上可约, 则存在 $F(X)$ 和 $G(X)\in\mathbb{C}(j)[X]$, 使得

$$\Phi_n(X)=F(X)G(X)=\prod_{i=1}^{\psi(n)}(X-j\circ\alpha_i),$$

故 $F(X)$ 和 $G(X)$ 均为某些 $(X-j\circ\alpha_i)$ 之积, 将 Γ 作用于 $\Phi_n(X)$ 上, 则知对任意 $\gamma\in\Gamma$, 有

$$\Phi_n(X)^\gamma=\Phi_n(X)=F(X)^\gamma G(X)^\gamma=\prod_{i=1}^{\psi(n)}(X-j\circ\alpha_i).$$

于是, 若 $\deg(F) \geqslant 1$, 则由 Γ 的可迁性, 知

$$F(X) = \prod_{i=1}^{\psi(n)} (X - j \circ \alpha_i) = \Phi_n(X),$$

故 $\Phi_n(X)$ 不可约.

其次, 证明 (ii) 的对称性. 我们可取 α_i 之一为 $\begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}$, 故 $j \circ \frac{1}{n}$ 是 $\Phi_n(X, j)$ 的一个根, 即

$$\Phi_n(j(\tau/n), j(\tau)) = 0, \qquad \forall\, \tau \in \mathfrak{H},$$

故

$$\Phi_n(j(\tau), j(n\tau)) = 0, \qquad \forall\, \tau \in \mathfrak{H}.$$

换言之, 即: $\Phi_n(j, j \circ n) = 0$, 故 $j \circ n$ 是 $\Phi_n(j, X)$ 的一个根. 但 $j \circ n$ 也是 $\Phi_n(X, j)$ 的一个根, 它对应于矩阵

$$\begin{pmatrix} n & 0 \\ 0 & 1 \end{pmatrix},$$

因 $\Phi_n(X, j)$ 是不可约的, 故有

$$\Phi_n(X, j) / \Phi_n(j, X).$$

即

$$\Phi_n(j, X) = g(X, j)\Phi_n(X, j)$$

对于某个多项式 $g(t, j) \in \mathbb{Z}[t, j]$ (Gauss 引理), 故

$$\Phi_n(j, X) = g(X, j)\Phi_n(X, j) = g(X, j)g(j, X)\Phi_n(j, X),$$

从而 $g(X, j)g(j, X) = 1$, $g(X, j) = \pm 1$. 若 $g(X, j) = -1$, 则 $\Phi_n(j, j) = -\Phi_n(j, j)$, 即 $\Phi_n(j, j) = 0$. 故 j 是 $\Phi_n(X)$ 的一个根, 但 $\Phi_n(X)$ 在 $\mathbb{Q}(j)$ 上是不可约的, 这不可能, 因此 $g(X, j) = 1$, (ii) 得证.

现证 (iii). 设 n 不是一个完全平方, 故若

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

α 本原, $ad=n$, 则 $a\neq d$, 我们有 q 展开式

$$j-j\circ\alpha=\frac{1}{q}+\cdots-\frac{1}{\zeta_d^b q^{a/d}}-\cdots,$$

因 $a\neq d$, 故没有极点项消去. 并且这个 q 展开式的首项系数是一个单位根. 但是 $\Phi_n(j,j)\in\mathbb{Z}[j]$. 取 $(j-j\circ\alpha_i)$ 的乘积, 我们看出 $\Phi_n(j,j)$ 的 q 展开式开始于

$$\frac{c_m}{q^m}+\cdots,$$

由于 c_m 必须为一个整数, 又必须是一个单位根, 故 $c_m\neq\pm1$.

$$\Phi_n(j,j)=c_m j^m+\cdots$$

是一个首项系数 $c_m=\pm1$ j 的整多项式, 证毕.

定理 2.14 (Kronecker同余关系) 设 p 为任意素数, 则模多项式 $\Phi_p(X,j)$ 满足下述同余关系式:

$$\Phi_p(X,j)\equiv(X-j^p)(X^p-j)\pmod p.$$

证明 对于一个素数 p, 行列式等于 p 的本原矩阵的代表元的一个完全集由下面给出:

$$\alpha_i=\begin{pmatrix}1&i\\0&p\end{pmatrix},\quad 0\leqslant i\leqslant p-1,\quad \alpha_p=\begin{pmatrix}p&0\\0&1\end{pmatrix}.$$

给定一个模函数 f, 记 $f^*(q)$ 是其 q 展开. 类似地, 有 $q^{1/N}$ 展开, 这样一个展开式是 $q^{1/N}$ 的一个幂级数. 如果 2 个 $q^{1/N}$ 展开的系数在环 $\mathbb{Z}[\zeta_p]$ 中 (此处 ζ_p 是 p 次单位根), 则关系式

$$f^*(q)\equiv g^*(q)\pmod{1-\zeta}$$

的意思是指: $f^*(q)-g^*(q)$ 的 $q^{1/N}$ 展开式中的所有系数都位于 $\mathbb{Z}[\zeta]$ 中 $1-\zeta$ 所生成的理想内.

由前面的讨论知, 若

$$\alpha=\begin{pmatrix}a&b\\0&d\end{pmatrix},$$

则

$$j\circ\alpha=\frac{1}{q^{a/d}\zeta_d^b}+P(q^{a/d}\zeta_d^b),\tag{2.22}$$

其中 P 是一个整系数的幂级数. 特别地, 有

$$(j\circ\alpha_p)^*(q)=\frac{1}{q^p}+P(q^p),\quad j^*(q)=\frac{1}{q}+P(q),\tag{2.23}$$

从而由 (2.23) 式知

$$(j\circ\alpha_p)^*(q)\equiv j^*(q)^p\pmod p,\tag{2.24}$$

而由 (2.22) 式

$$(j\circ\alpha_i)^*(q)=\frac{1}{q^{1/p}\zeta_p^i}+P(q^{1/p}\zeta_p^i),$$

可见

$$(j\circ\alpha_i)^*(q)\equiv j^*(q)^{1/p}\pmod{1-\zeta_p}.\tag{2.25}$$

由于 $1-\zeta_p$ 是 $\mathbb{Z}[\zeta_p]$ 中整除 p 的素元, 因此有

$$\Phi_p(X,j^*(q))\equiv(X-j^*(q)^p)(X^p-j^*(q))\pmod{1-\zeta_p},\tag{2.26}$$

这里的同余的意义如下：将左右两端均视为 X 的多项式, 则其系数是 q 的幂级数, 上述同余式的意思是这些对应的系数 (作为 q 的幂级数) 是按照我们前面给出的意义 $\bmod 1-\zeta_p$ 同余的. 这很容易推出 (利用 (2.24) 和 (2.25) 式)

$$\begin{aligned}\Phi_p(X,j^*(q))&=\prod_{i=0}^{p}\big(X-(j\circ\alpha_i)^*(q)\big)\\&=\big(X-(j\circ\alpha_p)^*(q)\big)\prod_{i=0}^{p-1}\big(X-(j\circ\alpha_i)^*(q)\big)\\&\equiv\big(X-j^*(q)^p\big)\prod_{i=0}^{p-1}\big(X-j^*(q)^{1/p}\big)\pmod{1-\zeta_p}\\&\equiv\big(X-j^*(q)^p\big)\big(X-j^*(q)^{1/p}\big)^p\pmod{1-\zeta_p}\\&\equiv(X-j^*(q)^p)(X^p-j^*(q))\pmod{1-\zeta_p}.\end{aligned}$$

现在令

$$\Phi_p(X,j)-(X-j^p)(X^p-j)=\sum_v\psi_v(j)X^v,\tag{2.27}$$

其中 $\psi_v(j)\in\mathbb{Z}[j]$. 于是由 (2.26) 式知 $\psi_v(j^*(q))$ 的系数被 $1-\zeta_p$ 除尽, 但 $\psi_v(j)\in\mathbb{Z}[j]$, $j^*(q)$ 是整系数幂级数, 从而 $\psi_v(j^*(q))$ 的系数是通常的有理整数, 于是 p 整除这些系数. 这就表明 $\psi_v(j)\equiv 0\pmod p$. 定理得证.

第三章　一般域上的椭圆曲线

在这一章我们利用纯代数的方法研究一般域上的椭圆曲线, 而不用上一章的复数域上的解析方法. 本章需应用一些代数曲线的知识, 读者可参阅文献 [12,14].

§3.1　椭圆曲线的群结构

Weierstrass 方程

设 K 为一个域, $\overline{K}$ 表示 K 的代数闭域. K 上的 Weierstrass 方程

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{3.1}$$

$(a_1, a_2, a_3, a_4, a_5, a_6 \in K)$ 决定射影平面 $\mathbb{P}^2(\overline{K})$ 上的一条曲线 E, 即适合上述方程的点 (X, Y, Z) $(X, Y, Z \in \overline{K})$ 的集合. 当该曲线非奇异时, 我们称它为定义在 K 上的椭圆曲线, 以 E/K 表示. 将方程 (3.1) 改写为形如 $F(X, Y, Z) = 0$, E 为非奇异是指 E 上不存在奇点, 即 E 上不存在使得 $\partial F/\partial X, \partial F/\partial Y$ 和 $\partial F/\partial Z$ 同时为零的点.

E 上有惟一的点 $(0, 1, 0)$ 具有坐标 $Z = 0$, 称该点为无穷远点, 记为 $\mathcal{O}$. 由于 $\partial F/\partial Z(\mathcal{O}) = 1$, 故 $\mathcal{O}$ 不是奇点. 当 $Z \neq 0$ 时, 令 $x = X/Z, y = Y/Z$, 方程 (3.1) 变为

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{3.2}$$

曲线 E 由方程 (3.2) 所有的解 (x, y) $(x, y \in \overline{K})$ 及无穷远点 $\mathcal{O}$ 组成. 将方程 (3.2) 表为 $f(x, y) = 0$ 的形式, E 上不存在使得 $\partial f/\partial x$ 和 $\partial f/\partial y$ 同时为零的点. E 上的每个点 (无穷远点除外) 都有射影坐标 (X, Y, Z) 和仿射坐标 (x, y) 两种表示方式.

当 K 的特征 $\mathrm{char}(K) \neq 2$ 时, 以 $y - a_1x/2 - a_3/2$ 代入方程 (3.2) 中的 y 得到

$$E: \quad y^2 = x^3 + \frac{b_2x^2}{4} + \frac{b_4x}{2} + \frac{b_4}{4}, \tag{3.3}$$

其中

$$b_2 = a_1^2 + 4a_2,$$
$$b_4 = 2a_4 + a_1a_3,$$
$$b_6 = a_3^2 + 4a_6.$$

当 $\mathrm{char}(K) \neq 2, 3$ 时, 在 (3.3) 式中再以 $x - b_2/12$ 代入 x 得到

$$E: \quad y^2 = x^3 + ax + b, \tag{3.4}$$

其中

$$a = -c_4/(3 \times 2^4), \qquad b = -c_6/(3^3 \times 2^5),$$

$$c_4 = b_2^2 - 24b_4, \qquad c_6 = b_2^3 + 36b_2b_4 - 216b_6.$$

定义 E 的两个重要参数

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6, \quad j = c_4^3/\Delta,$$

其中 Δ 称为 E 的判别式, j 称为 E 的 j 不变量, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$.

E 上没有奇点, 故 $f(x) = x^3 + ax + b = 0$ 没有重根, 即 $f(x)$ 与 $f'(x)$ 的结式 $4a^3 + 27b^2 \neq 0$. 通过直接计算可知 $\Delta = -16(4a^3 + 27b^2)$, 可见 E 为非奇异的充要条件是 $\Delta \neq 0$.

当 $\mathrm{char}(K) = 3$ 时, 将方程 (3.3) 改写为

$$E: \quad y^2 = x^3 + a_2x^2 + a_4x + a_6. \tag{3.5}$$

易见当且仅当 $\Delta = a_2^2a_4^2 - a_2^3a_6 - a_4^3 \neq 0$ 时, E 为非奇异. 若 (3.5) 式中 $a_2 = 0$, 则有

$$E: \quad y^2 = x^3 + a_4x + a_6, \quad \Delta = -a_4^3, \quad j = 0. \tag{3.6}$$

当 $a_2 \neq 0$ 时, 在 (3.5) 式中以 $x + a_4/a_2$ 代入 x, (3.5) 式化为

$$E: \quad y^2 = x^3 + a_2x^2 + a_6, \quad \Delta = -a_2^3a_6, \quad j = -a_2^3/a_6 \tag{3.7}$$

(我们约定 a_i 可以代表不同的值).

当 $\mathrm{char}(K) = 2$ 时, 方程 (3.2) 中若 $a_1 \neq 0$, 分别以 $a_1^2x + a_3/a_1$ 和 $a_1^3y + (a_1^2a_4 + a_3^2)/a_1^3$ 代入 x 和 y, 方程 (3.2) 化为

$$E: \quad y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6, \tag{3.8}$$

若 (3.2) 式中 $a_1 = 0$, 则以 $x + a_2$ 代入 x 得

$$E: \quad y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j = 0. \tag{3.9}$$

对于方程 (3.6) 至 (3.9) 定义的曲线, 可以分别验证当且仅当 $\Delta \neq 0$ 时, 它们为非奇异的.

椭圆曲线上的加法

方程 (3.1) 所定义的椭圆曲线 E 是射影平面 $\mathbb{P}^2(\overline{K})$ 上的一条 3 次曲线, 平面上任一直线与 E 都有 3 个交点 (不一定互不相同). 任取 E 上两点 P, Q, 连接 P, Q 的直线 (当 $P = Q$ 时, 取通过 P 的切线) 与 E 交于第 3 点 R, 我们将连接 R 与无穷远点 O 的直线与 E 的第 3 个交点记为 $P \oplus Q$. 在实数平面, 上述过程如图 3.1 所示.

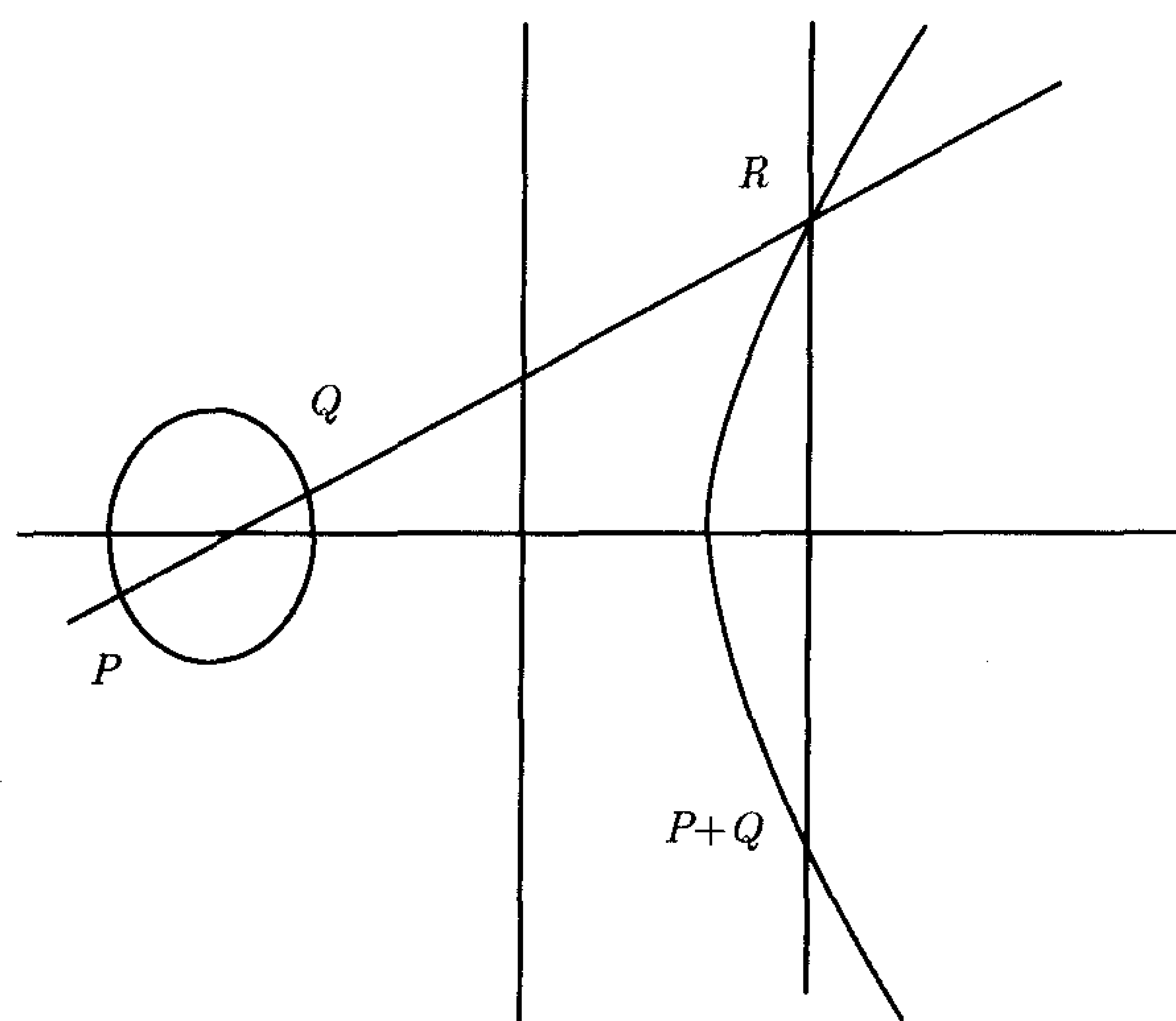


图 3.1 椭圆曲线上两个点的 $\oplus$ 运算

定理 3.1 运算 $\oplus$ 具有下述性质:

(1) 若直线 L 与 E 相交于 P,Q,R 三点, 则 $(P\oplus Q)\oplus R=\mathcal{O}$;

(2) 对任一 $P\in E$ 有 $P\oplus\mathcal{O}=P$;

(3) 对任意 $P,Q\in E$ 有 $P\oplus Q=Q\oplus P$;

(4) 对任一 $P\in E$, 存在 E 上一点, 表为 $\ominus P$, 使得 $P\oplus(\ominus P)=\mathcal{O}$;

(5) 设 $P,Q,R\in E$, 则 $(P\oplus Q)\oplus R=P\oplus(Q\oplus R)$.

换句话说, 运算 $\oplus$ 使得 E 成为一个交换群, 以下称它为 E 上的加法群, 并将 $\oplus,\ominus$ 分别改写为 $+,-$.

证明 (1) 将方程 (3.1) 改写为形如 $F(X,Y,Z)=0$, 易见 $\partial F/\partial X(\mathcal{O})=0,\partial F/\partial Y(\mathcal{O})=0,\partial F/\partial Z(\mathcal{O})=1$, E 与过 $\mathcal{O}$ 的切线 $Z=0$ 有惟一的交点 $\mathcal{O}$(三重交点). 由 $\oplus$ 的定义, 通过 $P\oplus Q$ 与 R 的直线交 E 于 $\mathcal{O}$, 而通过 $\mathcal{O}$ 的切线与 E 的第 3 个交点仍是 $\mathcal{O}$, 所以 (1) 得证.

(2) 设 R 为通过 P 与 $\mathcal{O}$ 的连线与 E 的第 3 个交点, 则通过 R 与 $\mathcal{O}$ 的连线交 E 于 P, 即有 $P\oplus\mathcal{O}=P$.

(3) 在 $\oplus$ 的定义中, P 与 Q 是对称的.

(4) 将 P 与 $\mathcal{O}$ 的连线与 E 的第 3 个交点记为 R, 利用 (1) 与 (2), 有

$$\mathcal{O}=(P\oplus\mathcal{O})\oplus R=P\oplus R,$$

即 $\ominus P=R$.

(5) 利用以下将推导的运算 $\oplus$ 的表达式, 再经过直接计算, 即可得到 $\oplus$ 的结合律, 证毕.

现在来推导 E 的加法运算表达式. 设定义 E 的方程为

$$f(x,y)=y^2+a_1xy+a_3y-x^3-a_2x^2-a_4x-a_6=0, \tag{3.10}$$

$P=(x_0,y_0)\in E$, 首先来推导 $-P$ 的表达式. 通过 P 与 $\mathcal{O}$ 的直线 $L:\ x=x_0$, L 与 E 的第 3 个交点即为 $-P$. 将 $x=x_0$ 代入 (3.10) 式得到 y 的 2 次方程 $f(x_0,y)=0$, 它的两个解即对应 L 与 E 的两个交点 $P=(x_0,y_0)$ 及 $-P=(x_0,y_0')$, 可见 $y_0+y_0'=-a_1x_0-a_3$, 所以 $-P=(x_0,-y_0-a_1x_0-a_3)$.

设 $P_1=(x_1,y_1)$ 及 $P_2=(x_2,y_2)$ 为 E 上两点. 当 $x_1=x_2, y_1+y_2+a_1x_1+a_3=0$ 时, $P_1+P_2=\mathcal{O}$. 当 $P_1+P_2\neq\mathcal{O}$ 时, 通过 P_1 与 P_2 的直线形如

$$L:\quad y=\lambda x+v,$$

若 $x_1\neq x_2$, 则 $\lambda=(y_1-y_2)/(x_1-x_2)$; 若 $x_1=x_2$, 由于 $P_1+P_2\neq\mathcal{O}$, 所以 $P_1=P_2$, L 为过 P_1 的切线, $\lambda=-\frac{\partial f}{\partial x}(P_1)/\frac{\partial f}{\partial y}(P_1)$. λ 确定后可得到 v. 记 L 与 E 的第三个交点为 $P_3=(x_3,y_3)$, 则 $P_1+P_2=-P_3$. 将 L 的方程代入 (3.10) 式得到

$$f(x,\lambda x+v)=(x-x_1)(x-x_2)(x-x_3),$$

由 $x_1+x_2+x_3=\lambda^2+a_1\lambda-a_2$ 可计算出 x_3 和 y_3.

***E* 的加法规则** 设 E 为由方程 (3.10) 定义的椭圆曲线.

(a) 设 $P=(x,y)\in E$, 则 $-P=(x,-y-a_1x-a_3)$; 令

$$P_1+P_2=P_3,\qquad P_i=(x_i,y_i)\in E,\quad i=1,2,3.$$

(b) 若 $x_1=x_2, y_1+y_2+a_1x_1+a_3=0$, 则 $P_1+P_2=\mathcal{O}$. 否则令

$$\lambda=\begin{cases}\dfrac{y_2-y_1}{x_2-x_1}, & \text{当 } x_1\neq x_2 \text{ 时},\\[2mm] \dfrac{3x_1^2+2a_2x_1+a_4-a_1y_1}{2y_1+a_1x_1+a_3}, & \text{当 } x_1=x_2 \text{ 时},\end{cases}$$

$$v=y_1-\lambda x_1.$$

(c) P_3 由下式给出：

$$x_3=\lambda^2+a_1\lambda-a_2-x_1-x_2,$$

$$y_3=\lambda(x_1-x_3)-y_1-a_1x_3-a_3.$$

特别地, 当 $P_1\neq P_2$ 时,

$$x(P_1+P_2)=\left(\frac{y_2-y_1}{x_2-x_1}\right)^2+a_1\left(\frac{y_2-y_1}{x_2-x_1}\right)-a_2-x_1-x_2,$$

当 $P_1 = P_2$ 时,

$$x(2P_1) = \frac{x_1^4 - b_4x_1^2 - 2b_6x_1 - b_8}{4x_1^3 + b_2x_1^2 + b_4x_1 + b_6},$$

其中 b_2, b_4, b_6, b_8 定义如前.

在实际应用中, 经常遇到以下两个特殊情形下的运算规则:

当 $\mathrm{char}(K) \neq 2, 3$ 时, 在方程 (3.4) 定义的 E 上, $-P = (x, -y)$. 当 $P_1 + P_2 \neq \mathcal{O}$ 时, 令

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{当 } x_1 \neq x_2 \text{ 时}, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{当 } x_1 = x_2 \text{ 时} \end{cases}$$

(当 $x_1 = x_2$ 时, 一定有 $y_1 \neq 0$, 否则 $P_1 = P_2 = -P_1$, 从而 $P_1 + P_2 = \mathcal{O}$), 则

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = \lambda(x_1 - x_3) - y_1.$$

方程 (3.4) 即为方程 (2.16). 正如在 (2.16) 式的前面所指出的, 以 y 替代 $y/2$, a 替代 $-g_2/4$, b 替代 $-g_3/4$, 方程 (2.1) 就变为 (3.4) 式, 所以将 §2.1 所给出的 (2.1) 式所定义的曲线上的运算规则, 经过上述同样的变换, 即得到这里的运算规则.

当 $\mathrm{char}(K) = 2$ 时, 在方程 (3.8) 定义的 E 上, $-P = (x, y + x)$, 当 $P_1 + P_2 \neq \mathcal{O}$ 时, 令

$$\lambda = \begin{cases} \dfrac{y_2 + y_1}{x_2 + x_1}, & \text{当 } x_1 \neq x_2 \text{ 时}, \\ \dfrac{x_1^2 + y_1}{x_1}, & \text{当 } x_1 = x_2 \text{ 时} \end{cases}$$

(同样当 $x_1 = x_2$ 时, 一定有 $x_1 \neq 0$), 则

$$x_3 = \lambda^2 + \lambda + a_2 + x_1 + x_2, \qquad y_3 = (x_1 + x_3)\lambda + y_1 + x_3.$$

同构与 j 不变量

设 E/K 为方程 (3.1) 定义的曲线, $\widehat{K}$ 为任一中间域, $K \subset \widehat{K} \subset \overline{K}$. (X, Y, Z) 为 E 上一点 $(X, Y, Z) \in \overline{K}$, 若存在 $\lambda \in \overline{K}$, 使得 $(\lambda X, \lambda Y, \lambda Z) \in \widehat{K}^3 \setminus \{(0, 0, 0)\}$, 则称 (X, Y, Z) 为 $\widehat{K}$ 上的有理点, 以 $E(\widehat{K})$ 表示 E 上全体 $\widehat{K}$ 有理点的集合, 由 E 上加法的定义, 可知 $E(\widehat{K})$ 成一个子群.

在方程 (3.1) 中作变换

$$\begin{aligned} \lambda: \quad & x = u^2x' + r, \\ & y = u^3y' + u^2sx' + t \end{aligned} \tag{3.11}$$

$(u, r, s, t \in \widehat{K}, u \neq 0)$, 得到同样由 Weirerstrass 方程定义的另一椭圆曲线

$$E': \quad y^2 + a_1'xy + a_3'y = x^3 + a_2'x^2 + a_4'x + a_6',$$

E 上的无穷远点变为 E' 上的无穷远点, 且

$$\begin{aligned}
ua_1' &= a_1 + 2s,\\
u^2a_2' &= a_2 - sa_1 + 3r - s^2,\\
u^3a_3' &= a_3 + ra_1 + 2t,\\
u^4a_4' &= a_4 - sa_3 + 2ra_2 - (t + rs)a_1 + 3r^2 - 2st,\\
u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1,\\
u^2b_2' &= b_2 + 12r,\\
u^4b_4' &= b_4 + rb_2 + br^2,\\
u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3,\\
u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4,\\
u^4c_4' &= c_4,\\
u^6c_6' &= c_6,\\
u^{12}\Delta' &= \Delta,\\
j' &= j.
\end{aligned} \tag{3.12}$$

定理 3.2 当且仅当 $\Delta \neq 0$ 时, 方程 (3.1) 定义的曲线 E 是非奇异的.

证明 变换 λ 建立了曲线 E 与 E' 的点之间的一一对应, 且 E 的奇点与 E' 的奇点互相对应. 对于方程 (3.4) 和 (3.6)~(3.9) 所定义的曲线, 通过直接验算, 已经证明了当且仅当 $\Delta \neq 0$ 时为非奇异, 这些曲线都由曲线 E 通过形如 λ 的变换产生, 且已包含了所有可能的情形, 由此可见定理 3.2 成立, 证毕.

λ 变换将射影平面 $\mathbb{P}^2(\widehat{K})$ 上的直线变为直线, 由椭圆曲线加法的定义, 可见 λ 保持加法不变, 即

$$\lambda(P + Q) = \lambda(P) + \lambda(Q) \quad (P, Q \in E).$$

我们称 λ 是 $E(\widehat{K})$ 与 $E'(\widehat{K})$ 定义在 $\widehat{K}$ 上的同构 (在通常加法群意义下的同构). (3.12) 式表示 $\widehat{K}$ 上同构的椭圆曲线具有相同的 j 不变量 (这也就是该名称的由来). 进一步可以证明

定理 3.3 定义在 K 上的两条椭圆曲线在 $\overline{K}$ 上同构, 当且仅当它们具有相同的 j 不变量.

证明　(3.12) 式表明在 $\overline{K}$ 上同构的椭圆曲线具有相同的 j 不变量, 所以仅需证明具有相同 j 不变量的曲线一定在 $\overline{K}$ 上同构. 我们只要对 (3.4) 和 (3.6)~(3.9) 式定义的曲线分别证明上述结论即可. 这里仅以讨论 (3.4) 式定义的曲线为例. 设

$$E: \quad y^2 = x^3 + ax + b, \qquad E': \quad y^2 = x^3 + a'x + b'$$

具有相同的 j 不变量, 则由 j 的定义得

$$j = 3^3 \cdot 2^8 a^3/(4a^3 + 27b^2) = 3^3 \cdot 2^8 (a')^3/(4(a')^3 + 27(b')^2)$$

$(4a^3 + 27b^2 \neq 0,\ \ 4a'^3 + 27b'^2 \neq 0)$, 由此可得 $a^3 b'^2 = a'^3 b^2$ 分别以下面 3 种情形构造 E 与 E' 的同构 $(x, y) = (u^2 x', u^3 y')$:

(1) $a = 0\ \ (j = 0)$, 这时 $b \neq 0, a' = 0, b' \neq 0$, 取 $u = (b/b')^{1/6}$;

(2) $b = 0\ \ (j = 1728)$, 这时 $a \neq 0, b' = 0, a' \neq 0$, 取 $u = (a/a')^{1/4}$;

(3) $ab \neq 0\ \ (j \neq 0, 1728)$, 这时 $a'b' \neq 0$, 取 $u = (a/a')^{1/4} = (b/b')^{1/6}$.

定理证毕.

§3.2　除子类群

设 E/K 为椭圆曲线, E 上的点生成的形式和 (不是 §3.1 中定义的加法)

$$D = \sum_{P \in E} n_P (P)$$

称为 E 的一个除子, 这里 n_P 为整数, 且对几乎所有的 $P \in E(\overline{K})$, 有 $n_P = 0$. 所有除子按这种形式加法形成一个自由交换群, 称为 E 的除子群, 记为 $\mathrm{Div}(E)$. 除子 D 的次数 $\deg D$ 定义为

$$\deg D = \sum_{P \in E} n_P.$$

所有次数为零的除子组成 $\mathrm{Div}(E)$ 的一个子群, 记为 $\mathrm{Div}^{\circ}(E)$.

设 $f(x, y) = 0\ \ (f \in K[x, y])$ 为定义 E 的方程, $f(x, y)$ 生成 $\overline{K}[x, y]$ 中一个素理想, 整环 $\overline{K}[x, y]/(f(x, y))$ 的商域称为 E 的函数域, 记为 $\overline{K}(E)$(类似地可以定义 E 在 K 上的函数域 $K(E)$). $\overline{K}(E)$ 中的任一函数可表为 $h_1(X, Y, Z)/h_2(X, Y, Z)$, h_1 和 h_2 是次数相同的两个齐次多项式, 且 h_2 不在 E 上恒为零.

设 $g \in \overline{K}(E)^*$($\overline{K}(E)$ 的非零元集合), 定义 g 所对应的除子

$$\mathrm{div}(g) = \sum_{P \in E} \mathrm{ord}_P(g)(P),$$

这里 $\mathrm{ord}_P(g)$ 是 g 在 P 的阶 (因 P 是光滑点, $\mathrm{ord}_P(g)$ 是有定义的), 当 $\mathrm{ord}_P(g)>0$ 时, 表示 P 是 g 的 $\mathrm{ord}_P(g)$ 阶零点, 当 $\mathrm{ord}_P(g)<0$ 时, 表示 P 是 g 的 $-\mathrm{ord}_P(g)$ 阶极点. g 仅有有限个零点和极点, 对任一 $g\in\overline{K}(E)$ 都有 $\deg(\mathrm{div}(g))=0$ (见以下的推论 3.2).

$\overline{K}(E)$ 中任一函数 g 对应的除子 $\mathrm{div}(g)$ 称为主除子, 所有主除子形成 $\mathrm{Div}(E)$ 的一个子群, $\mathrm{Div}(E)$ 对它的商群称为除子类群 (或 Picard 群), 记为 $\mathrm{Pic}(E)$. 两个除子 D_1 和 D_2, 若存在 $g\in\overline{K}(E)$, 使得 $D_2=D_1+\mathrm{div}(g)$, 则称 D_1 与 D_2 线性等价, 记为 $D_1\sim D_2$, 这时有 $\deg D_1=\deg D_2$. $\mathrm{Div}^\circ(E)$ 关于主除子群的商群记为 $\mathrm{Pic}^\circ(E)$.

记 P 和 Q 为 E 上两点, 通过 P 和 Q 的直线记为 $L_1=0$, 它与 E 交于第 3 点 R, 通过 R 与无穷远点 $\mathcal{O}$ 的直线 $L_2=0$ 与 E 交于第 3 点, 即为 $P+Q$, 直线 $Z=0$ 与 E 在 $\mathcal{O}$ 点相切, 且重数为 3, 故

$$\mathrm{div}(L_1/Z)=(P)+(Q)+(R)-3(\mathcal{O}),\mathrm{div}(L_2/Z)=(R)+(P+Q)-2(\mathcal{O}),$$

所以

$$\begin{aligned}\mathrm{div}(L_1/L_2)&=\mathrm{div}(L_1/Z)-\mathrm{div}(L_2/Z)\\&=(P)+(Q)-(P+Q)-(\mathcal{O}),\end{aligned}$$

这里 $L_1/Z,L_2/Z,L_1/L_2$ 都为 $\overline{K}(E)$ 中的函数, 由此可见

$$(P)-(\mathcal{O})+(Q)-(\mathcal{O})\sim(P+Q)-(\mathcal{O}). \tag{3.13}$$

设 $D=\sum n_P(P)$ 为 $\mathrm{Div}^\circ(E)$ 中任一除子, 即 $\sum n_P=0$, 反复利用 (3.13) 式可以发现

$$D=\sum n_P\big((P)-(\mathcal{O})\big)\sim\Big(\sum n_PP\Big)-(\mathcal{O}), \tag{3.14}$$

和式 $\sum n_PP$ 为 E 上的加法. (3.14) 式表示 $\mathrm{Div}^\circ(E)$ 中任一除子都与形如 $(P)-(\mathcal{O})$ 的除子线性等价, 亦即映射

$$\begin{aligned}\kappa:\ \ E&\longrightarrow \mathrm{Pic}^\circ(E)\\P&\longmapsto(P)-(\mathcal{O})\end{aligned}$$

是一个群同态, 且是满射.

以下用 Riemann-Roch 定理证明 κ 是一个单射, 亦即 κ 是一个同构.

设 $D\in\mathrm{Div}(E)$, 定义函数集

$$\mathscr{L}(D)=\{g\in\overline{K}(E)^*\,|\,\mathrm{div}(g)\geqslant-D\}\bigcup\{0\},$$

$\mathscr{L}(D)$ 是 $\overline{K}$ 上的有限维线性空间 (见文献 [14], II 5.19), 其维数记为 $l(D)$, 由于对任一 $g\in\overline{K}(E)^*$ 有 $\deg\big(\mathrm{div}(g)\big)=0$, 可见当 $\deg(D)<0$ 时, 有 $l(D)=0$.

对任一非奇异曲线 $\mathcal{C}$, 可类似地定义 $\mathrm{Div}(\mathcal{C})$.

定理 3.4 (Riemann-Roch 定理)　设 $\mathcal{C}$ 为非奇异曲线, 则存在 $\mathcal{C}$ 的一个除子 $K_{\mathcal{C}}$(称为典范除子) 和一个整数 $g \geqslant 0$(称为亏格), 使得对任一 $D \in \mathrm{Div}(\mathcal{C})$ 有

$$l(D) - l(K_{\mathcal{C}} - D) = \deg(D) - g + 1. \tag{3.15}$$

引理 3.1　(a) $l(K_{\mathcal{C}}) = g$,

(b) $\deg(K_{\mathcal{C}}) = 2g - 2$,

(c) 若 $\deg(D) > 2g - 2$, 则 $l(D) = \deg(D) - g + 1$.

证明　(a) 在 (3.15) 式中取 $D = 0$, 由定义可知 $l(0) = 1$, 故得 $l(K_{\mathcal{C}}) = g$.

(b) 在 (3.15) 式中取 $D = K_{\mathcal{C}}$, 利用 (a) 可得 $\deg(K_{\mathcal{C}}) = 2g - 2$.

(c) 由于 $\deg(K_{\mathcal{C}} - D) < 0$, 故 $l(K_{\mathcal{C}} - D) = 0$, 利用 (3.15) 式即证.

椭圆曲线是亏格 $g = 1$ 的非奇异曲线 (事实上, 可以证明任一非奇异且亏格为 1 的曲线都是由 Weierstrass 方程 (3.1) 所定义, 见文献 [12]). 利用 Riemann-Roch 定理可证明

命题 3.1　设 P 和 Q 为 E 上两点, 则 $(P) \sim (Q)$ 当且仅当 $P = Q$.

证明　假设 $(P) \sim (Q)$, 则存在 $f \in \overline{K}(E)$, 使得

$$\mathrm{div}(f) = (P) - (Q),$$

故 $f \in \mathscr{L}(Q)$. 因 $\deg(Q) = 1$, 由引理 3.1(c) 有 $l\big((Q)\big) = 1$. 显然 $\mathscr{L}(Q)$ 包含所有常数函数, 从而 $\mathscr{L}(\theta) = \overline{K}$, 亦即 $f \in \overline{K}$, 所以 $P = Q$, 证毕.

于是我们有

定理 3.5　椭圆曲线 E 与 $\mathrm{Pic}^{\circ}(E)$ 有同构映射

$$\begin{aligned} \kappa:\ & E \xrightarrow{\sim} \mathrm{Pic}^{\circ}(E) \\ & P \longmapsto (P) - (\mathcal{O}). \end{aligned}$$

若 $D = \sum n_P(P) \in \mathrm{Pic}^{\circ}(E)$, 则 $\kappa^{-1}(D) = \sum n_P P$(为 E 上求和).

推论 3.1　除子 $D = \sum n_P(P)$ 为主除子的充要条件为 $\sum n_P = 0$ 及 $\sum n_P P = \mathcal{O}$.

§3.3　同种映射

设 E_1/K 和 E_2/K 为两条椭圆曲线, ϕ 为从 E_1 到 E_2 的有理映射

$$\begin{aligned} \phi:\quad & E_1 \longrightarrow E_2 \\ & (X, Y, Z) \longmapsto (f_1(X, Y, Z), f_2(X, Y, Z), f_3(X, Y, Z)), \end{aligned}$$

其中 $f_1, f_2, f_3 \in \overline{K}(E_1)$. E_1 为非奇异曲线, 对任一 $P \in E_1$, 一定存在 $g \in \overline{K}(E_1)$, 使得 gf_i $(i=1,2,3)$ 在 P 点都有意义, 这时 $(gf_1(P), gf_2(P), gf_3(P)) \in E_2$, 即 ϕ 在 E_1 的任一点都有意义. 当 ϕ 不是常值映射时, ϕ 一定是映上的 (见文献 [14], 第二章定理 6.8).

ϕ 诱导出从 $\overline{K}(E_2)$ 到 $\overline{K}(E_1)$ 的一个同态映射

$$\begin{aligned} \phi^*: \quad & \overline{K}(E_2) \longrightarrow \overline{K}(E_1) \\ & f \quad \longmapsto f \cdot \phi, \end{aligned}$$

当 ϕ 不是常值映射时, $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的有限扩张, (文献 [14], 第二章定理 6.8), 定义 ϕ 的次数为

$$\deg \phi = [\overline{K}(E_1) : \phi^*(\overline{K}(E_2))].$$

当 ϕ 为常值映射时, 令 $\deg \phi = 0$. 当 $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的可分、不可分、纯不可分扩张时, ϕ 也相应地称为可分、不可分、纯不可分.

命题 3.2 设 $\tau: \overline{K}(E_2) \to \overline{K}(E_1)$ 为嵌入映射, 则存在有理映射 ϕ: $E_1 \to E_2$, 使得 $\phi^* = \tau$.

证明 设定义 E_1 的方程为 $f_1(x,y)=0$, $x, y \in \overline{K}(E_1)$. 定义 E_2 的方程为 $f_2(X, Y)=0$, $X, Y \in \overline{K}(E_2)$, $\tau(X)$, $\tau(Y)$ 都是 x 和 y 的有理函数, $\phi(x,y) = \big(\tau(X), \tau(Y)\big)$ 是 $E_1 \to E_2$ 的有理映射 (显然有 $f_2\big(\tau(X), \tau(Y)\big) = \tau\big(f_2(X,Y)\big) = 0$), 对任一 $g(X,Y) \in \overline{K}(E_2)$, $\phi^* g = g\big(\tau(X), \tau(Y)\big) = \tau \cdot g$, 故 $\phi^* = \tau$, 证毕.

ϕ 也诱导出从 $\overline{K}(E_1)$ 到 $\overline{K}(E_2)$ 的一个同态映射

$$\begin{aligned} \phi_*: \quad & \overline{K}(E_1) \longrightarrow \overline{K}(E_2) \\ & f \quad \longmapsto (\phi^*)^{-1} N_{\overline{K}(E_1)/\phi^*(\overline{K}(E_2))}(f), \end{aligned}$$

这里 N 是从 $\overline{K}(E_1)$ 到 $\phi^*(\overline{K}(E_2))$ 的范映射.

设 P 为 E_1 的任一点, 则存在 $t_P \in \overline{K}(E_1)$, 使得 $\mathrm{ord}_P(t_P) = 1$, 函数 t_P 称为 P 的单值化子. 设 $t_{\phi(P)} \in \overline{K}(E_2)$ 为 $\phi(P)$ 的单值化子, 定义

$$e_\phi(P) = \mathrm{ord}_P(\phi^* t_{\phi(P)})$$

为 ϕ 在 P 的分歧指数, 对任一 $Q \in E_2$, 有 (文献 [14], 第二章定理 6.9)

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi. \tag{3.16}$$

引理 3.2 设 $\phi: \mathcal{C}_1 \to \mathcal{C}_2$, $\psi: \mathcal{C}_2 \to \mathcal{C}_3$ 均为非常值的有理映射, 对任一 $P \in \mathcal{C}_1$ 有

$$e_{\psi \cdot \phi}(P) = e_\phi(P) e_\psi\big(\phi(P)\big).$$

证明　设 $t_{\phi(P)}$ 和 $t_{\psi\phi(P)}$ 分别为 $\phi(P)$ 和 $\psi\phi(P)$ 的单值化子. 由于 $e_\psi(\phi(P)) = \mathrm{ord}_{\phi(P)}(\psi^* t_{\psi(\phi(P))})$, 故 $\psi^* t_{\psi\phi(P)}$ 与 $t_{\phi(P)}^{e_\psi(\phi(P))}$ 在 $\phi(P)$ 有同样的阶, 因而

$$\begin{aligned} e_\phi(P)e_\psi(\phi(P)) &= \mathrm{ord}_P\left(\phi^* t_{\phi(P)}^{e_\psi(\phi(P))}\right) = \mathrm{ord}_P\left(\phi^* \cdot \psi^* t_{\psi\phi(P)}\right) \\ &= \mathrm{ord}_P\left((\psi\phi)^* t_{\psi\phi(P)}\right) = e_{\psi\phi(P)}. \end{aligned}$$

证毕.

考虑 E_1 和 E_2 上的除子类群, ϕ 在 $\mathrm{Div}(E_1)$ 和 $\mathrm{Div}(E_2)$ 之间诱导两个映射 (仍记为 ϕ^* 和 ϕ_*)

$$\begin{aligned} \phi^*: \quad \mathrm{Div}(E_2) &\longrightarrow \mathrm{Div}(E_1) \\ (Q) &\longmapsto \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P), \end{aligned}$$

及

$$\begin{aligned} \phi_*: \quad \mathrm{Div}(E_1) &\longrightarrow \mathrm{Div}(E_2) \\ (P) &\longmapsto (\phi(P)). \end{aligned}$$

命题 3.3　*设 C_1 和 C_2 为非奇异曲线, ϕ 为 $C_1 \to C_2$ 的非常值有理映射, 类似地定义 $e_\phi(P), \phi^*, \phi_*$, 则*

(a) *对所有的 $D \in \mathrm{Div}(C_2)$, $\deg(\phi^* D) = (\deg\phi)(\deg D)$;*

(b) *对所有的 $f \in \overline{K}(C_2)^*$, $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$;*

(c) *对所有的 $D \in \mathrm{Div}(C_1)$, $\deg(\phi_* D) = \deg D$;*

(d) *对所有的 $f \in \overline{K}(C_1)^*$, $\phi_*(\mathrm{div}(f)) = \mathrm{div}(\phi_* f)$.*

证明　(a) 设 $D = \sum n_Q(Q)$, 则

$$\phi^* D = \sum_Q n_Q \cdot \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P),$$

由 (3.16) 式得

$$\deg(\phi^* D) = \sum_Q n_Q \sum_{P\in\phi^{-1}(Q)} e_\phi(P) = (\deg\phi)(\deg D).$$

(b) 我们有

$$\begin{aligned} \phi^*(\mathrm{div}(f)) &= \phi^*\Big(\sum_Q \mathrm{ord}_Q(f)(Q)\Big) \\ &= \sum_Q \mathrm{ord}_Q(f) \sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P) \\ &= \sum_P \mathrm{ord}_P(\phi^* t_{\phi(P)})\mathrm{ord}_{\phi(P)}(f)(P) \\ &= \sum_P \mathrm{ord}_P(\phi^* f)(P) = \mathrm{div}(\phi^* f). \end{aligned}$$

(c) 利用 ϕ_* 的定义即证.

(d) 见文献 [11], 第一章, 命题 22.

推论 3.2 对任一非常数的函数 $g \in \overline{K}(E)$, 有 $\deg(\mathrm{div}(g)) = 0$.

证明 以 $\mathbb{P}_1$ 表示射影直线, $\mathbb{P}_1$ 上的无穷远点记为 ∞. 定义有理映射

$$\begin{aligned} g: \quad & E \longrightarrow \mathbb{P}_1 \\ & P \longmapsto g(P), \end{aligned}$$

易见 $\mathrm{div}(g) = g^*\big((0) - (\infty)\big)$, 由命题 3.3(a) 得 $\deg\big(\mathrm{div}(g)\big) = 0$, 证毕.

由命题 3.3(a) 及 (c) 可见 ϕ^* 将 $\mathrm{Div}^\circ(E_2)$ 映入 $\mathrm{Div}^\circ(E_1)$, ϕ_* 将 $\mathrm{Div}^\circ(E_1)$ 映入 $\mathrm{Div}^\circ(E_2)$. 由命题 3.3(b) 及 (d) 可见 ϕ^* 将主除子映为主除子. ϕ_* 也将主除子映为主除子, 所以 ϕ^* 和 ϕ_* 分别诱导同态映射

$$\phi^*: \quad \mathrm{Pic}^\circ(E_2) \longrightarrow \mathrm{Pic}^\circ(E_1),$$

和

$$\phi_*: \quad \mathrm{Pic}^\circ(E_1) \longrightarrow \mathrm{Pic}^\circ(E_2).$$

设 ϕ 为 E_1 到 E_2 的有理映射, 若 $\phi(\mathcal{O}) = \mathcal{O}$, 则称 ϕ 为同种映射.

定理 3.6 设 $\phi: \ E_1 \to E_2$ 为同种映射, 则它是同态映射, 即对所有 $P, Q \in E_1$, 有

$$\phi(P+Q) = \phi(P) + \phi(Q).$$

证明 我们有群同构 (定理 3.5)

$$\begin{aligned} \kappa_i: \quad & E_i \longrightarrow \mathrm{Pic}^\circ(E_i) \\ & P \longmapsto (P) - (\mathcal{O}) \end{aligned}$$

$(i = 1, 2)$. 由于 $\phi(\mathcal{O}) = \mathcal{O}$, 下列图是可交换的:

$$\begin{array}{ccc} E_1 & \xrightarrow{\kappa_1} & \mathrm{Pic}^\circ(E_1) \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi_*} \\ E_2 & \xrightarrow{\kappa_2} & \mathrm{Pic}^\circ(E_2) \end{array}$$

因 κ_1 和 κ_2 是同构映射, ϕ_* 是同态映射, 故 ϕ 也是同态映射.

将 E_1 到 E_2 所有的同种映射形成的加法群记为 $\mathrm{Hom}(E_1, E_2)$. 当 $E_1 = E_2$ 时, 记 $\mathrm{End}(E) = \mathrm{Hom}(E, E)$. 若 $\phi, \psi \in \mathrm{End}(E)$, 将 $\phi\psi$ 理解为 ϕ 与 ψ 的复合映射, 于是 $\mathrm{End}(E)$ 成为一个环, 称为 E 的自同态环. 任一整数 m, 对应 $\mathrm{End}(E)$ 中一个同种映射: $P \mapsto mP$, 将它表示为 $[m]$. 易见对任一 $\phi \in \mathrm{End}(E)$, 有 $\phi \cdot [m] = [m] \cdot \phi$. Frobenius 映射是另一类重要的同种映射 (当 $\mathrm{char}(K) > 0$ 时).

Frobenius 映射

设 $\mathrm{char}(K)=p>0,\ \ q=p^r,\ \ E/K$ 为方程 (3.1) 定义的曲线, 以 $E^{(q)}$ 表示由方程

$$Y^2Z+a_1^qXYZ+a_3^qYZ^2=X^3+a_2^qX^2Z+a_4^qXZ^2+a_6^qZ^3$$

定义的曲线, 则映射

$$\phi_q:\quad (x,y,z)\longmapsto(x^q,y^q,z^q)$$

将 E 映为 $E^{(q)}$, 且 $\phi_q(\mathcal{O})=\mathcal{O}$, 所以 $\phi_q\in\mathrm{Hom}(E,E^{(q)})$, 称为 Frobenius 映射.

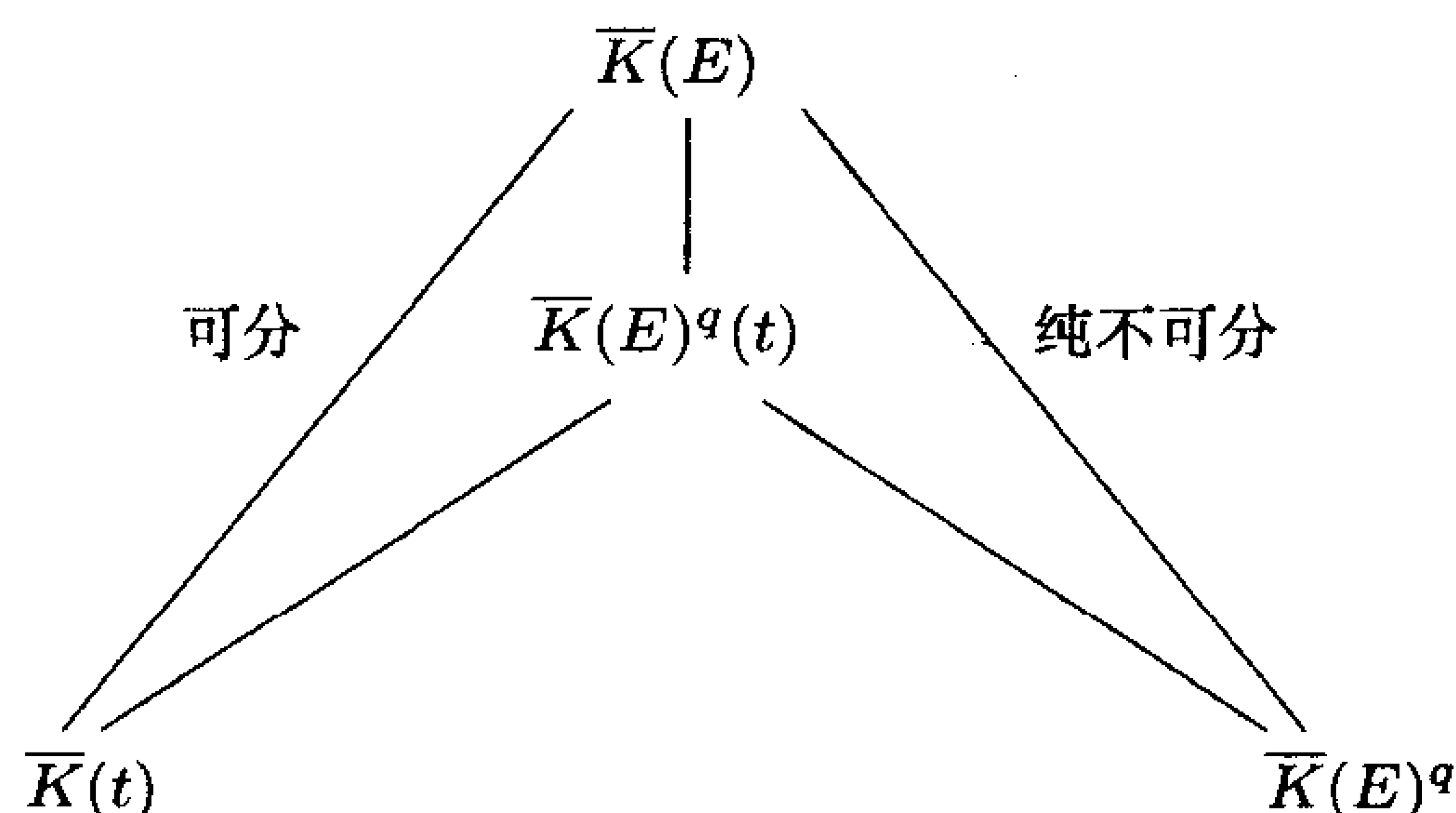
设 $h(X,Y,Z)/g(X,Y,Z)\in\overline{K}(E^{(q)})$, 其中 h 和 g 为次数相同的齐次多项式, 则

$$\begin{aligned}\phi_q^*(h/g)&=h(X^q,Y^q,Z^q)/g(X^q,Y^q,Z^q)\\&=(h'(X,Y,Z)/g'(X,Y,Z))^q,\end{aligned}$$

h' 和 g' 为分别将 h 和 g 的系数开 q 次方得到, 可见 $\phi_q^*(\overline{K}(E^{(q)}))=\big(\overline{K}(E)\big)^q$, 因而域扩张 $\overline{K}(E)/\phi_q^*(\overline{K}(E^{(q)}))$ 是纯不可分扩张, 即 ϕ_q 是纯不可分的, 进一步有

定理 3.7　*ϕ_q 是纯不可分的, 且 $\deg\ \ \phi_q=q$.*

证明　仅需证明后一结论. 任取 $P\in E$, 设 $t\in\overline{K}(E)$ 为 P 点的单值化子, 则 $\overline{K}(E)/\overline{K}(t)$ 是可分扩张 (见文献 [12], 第二章, 命题 1.4]). 考虑域塔



可知 $\overline{K}(E)=\overline{K}(E)^q(t)$, 从而 $\deg\phi_q=[\overline{K}(E)^q(t):\overline{K}(E)^q]$, 由于 $t^q\in\overline{K}(E)^q$, 为了证明 $\deg\phi_q=q$, 仅需证明 $t^{q/p}\notin\overline{K}(E)^q$.

反之, 若存在 $f\in\overline{K}(E)$, 使得 $t^{q/p}=f^q$, 则

$$q/p=\mathrm{ord}_p(t^{q/p})=q\cdot\mathrm{ord}_p(f),$$

这不可能, 证毕.

设 $\phi\in\mathrm{Hom}(E_1,E_2)$, ϕ 为群同态, 故 $\mathrm{Ker}\phi=\phi^{-1}(\mathcal{O})$, 且对任一 $Q\in E_2$ 有

$$\#\phi^{-1}(Q)=\#\phi^{-1}(\mathcal{O})=\#\mathrm{Ker}\phi.$$

由 (3.16) 式, 可知 $\#\mathrm{Ker}\phi\leqslant\deg\phi$. 进一步可以证明

定理 3.8 设 $\phi \in \mathrm{Hom}(E_1, E_2)$, 则 $\#\mathrm{Ker}\phi = \deg_s \phi$, 且对任一 $P \in E_1$ 有 $e_\phi(P) = \deg_i \phi$, 这里 $\deg_s \phi$ 和 $\deg_i \phi$ 分别表示扩张 $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ 的可分次数和不可分次数.

证明 对几乎所有的 $Q \in E_2$ 有 $\#\phi^{-1}(Q) = \deg_s \phi$(见文献 [14], 第二章定理 6.8). 任取 $Q, Q' \in E_2$, 存在 $R \in E_1$, 使得 $\phi(R) = Q' - Q$. 因 ϕ 是同态映射, 所以

$$\begin{aligned} \phi^{-1}(Q) &\longrightarrow \phi^{-1}(Q') \\ P &\longmapsto P + R \end{aligned}$$

是一一映射, 所以对所有 $Q \in E_2$ 有 $\#\phi^{-1}(Q) = \deg_s \phi$, 显然 $\#\mathrm{Ker}\phi = \deg_s \phi$.

设 $P, P' \in E_1$, $\phi(P) = \phi(P') = Q$, 令 $R = P' - P$, 易见 $\phi(R) = \mathcal{O}$, 定义 E_1 上的有理变换 $\tau_R(S) = S + R(\forall S \in E_1)$, τ_R^* 是 $\overline{K}(E_1)$ 的同构, 故 $\deg \tau_R = 1$, 从而对任一 $P \in E_1$ 有 $e_{\tau_R}(P) = 1$((3.16) 式). 由于 $\phi \cdot \tau_R = \phi$ 及引理 3.2,

$$e_\phi(P) = e_{\phi \cdot \tau_R}(P) = e_{\tau_R}(P) e_\phi\big(\tau_R(P)\big) = e_\phi(P'),$$

即 $\phi^{-1}(Q)$ 中每一点的分歧指数相同. 再由 (3.16) 式得

$$\begin{aligned} \deg_s(\phi) \deg_i \phi = \deg \phi &= \sum_{P \in \phi^{-1}(Q)} e_\phi(P) \\ &= \big(\#\phi^{-1}(Q)\big) \cdot e_\phi(P) = \deg_s \phi \cdot e_\phi(\phi), \end{aligned}$$

即证.

设 $\phi \in \mathrm{Hom}(E_1, E_2)$, $T \in \mathrm{Ker}\phi$, 定义 E_1 上的有理变换

$$\tau_T(P) = T + P, \qquad \forall P \in E_1,$$

τ_T 诱导 $\overline{K}(E_1)$ 一个同构

$$\tau_T^*(f)(P) = f(T + P), \qquad \forall f \in \overline{K}(E_1).$$

当 $f = g \cdot \phi \quad (g \in \overline{K}(E_2))$ 时,

$$\tau_T^*(f)(P) = g(\phi(T + P)) = g(\phi(P)) = f(P),$$

所以 $\tau_T^*(f) = f$, 即 $\phi^*(\overline{K}(E_2))$ 包含在 τ_T^* 的固定子域内.

定理 3.9 设 $\phi \in \mathrm{Hom}(E_1, E_2)$, 映射

$$\begin{aligned} \mathrm{Ker}\phi &\longrightarrow \mathrm{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \\ T &\longmapsto \tau_T^* \end{aligned}$$

是一个同构, 当 ϕ 可分时, $\overline{K}(E_1)/\phi^*(\overline{K}(E_2))$ 是 Galois 扩张, 其 Galois 群与 $\mathrm{Ker}\phi$ 同构.

证明　若 $T, S \in \mathrm{Ker}\phi$, 易见 $\tau^*_{(S+T)} = \tau^*_T \cdot \tau^*_S$, 由定理 3.6, 有 $\#\mathrm{Ker}\phi = \deg_s \phi$, 由 Galois 理论有 $\#\mathrm{Aut}[\overline{K}(E_1)/\phi^*(\overline{K}(E_2))] \leqslant \deg_s \phi$, 所以仅需证明映射 $T \mapsto \tau^*_T$ 是一个单射. 假设 τ^*_T 是一个恒等变换, 则对任一 $f \in \overline{K}(E_1)$, 都有 $f(\mathcal{O}) = f(T)$, 显然这时有 $T = \mathcal{O}$. 当 ϕ 可分时有 $\#\mathrm{Ker}\,\phi = \deg\,\phi$, 即

$$\#\mathrm{Aut}[\overline{K}(E_1)/\phi^*\overline{K}(E_2))] = \deg \phi,$$

定理得证.

定理 3.10　设 E_1, E_2, E_3 为定义在 K 上的椭圆曲线, $\phi:\ E_1 \to E_2$, $\psi:\ E_1 \to E_3$ 为非常值的同种映射, ϕ 可分. 若 $\mathrm{Ker}\phi \subset \mathrm{Ker}\psi$, 则存在惟一的同种映射 $\lambda:\ E_2 \to E_3$, 使得 $\psi = \lambda \circ \phi$.

证明　ϕ 可分, 故 $\overline{K}(E_1)$ 是 $\phi^*(\overline{K}(E_2))$ 的 Galois 扩张 (定理 3.9). 由于 $\mathrm{Ker}\phi \subset \mathrm{Ker}\psi$, 所以 $\psi^*(\overline{K}(E_3))$ 是 $\mathrm{Gal}(\overline{K}(E_1)/\phi^*(\overline{K}(E_2)))$ 的一个固定子域, 且有 $\psi^*(\overline{K}(E_3)) \subset \phi^*(\overline{K}(E_2)) \subset \overline{K}(E_1)$. 由命题 3.2, 存在 $\lambda:\ E_2 \to E_3$, 使得 $\phi^*(\lambda^*\overline{K}(E_3)) = \psi^*(\overline{K}(E_2))$, 可见 $\psi = \lambda \cdot \phi$. 由于 $\lambda(\mathcal{O}) = \lambda(\phi(\mathcal{O})) = \psi(\mathcal{O}) = \mathcal{O}$, 故 λ 是同种映射. λ 的惟一性是显然的, 证毕.

微分

现在讨论曲线上的微分所组成的向量空间. 它有两个作用, 其一是传统的微分所具有的线性化的作用 (见以下命题 3.8), 另一个作用是用于判断曲线之间的一个有理映射是否可分 (见以下命题 3.6). 这后一作用也是传统的微分所具有的, 一个域的扩张是可分的, 当且仅当每个元素的极小多项式的微分不为零.

设 E 为 $\overline{K}$ 上方程 (3.2) 所定义的椭圆曲线, 将此方程记为 $f(x,y) = 0$, $\overline{K}(E) = \overline{K}[x,y]/(f(x,y)) = \overline{K}(x)(y)$ 为 E 的函数域.

定义 3.1　对 $\overline{K}(E)$ 中任一函数 g, 定义符号 dg 具有以下性质:

(i) $d(x+y) = dx + dy$, 任意 $x, y \in \overline{K}(E)$;

(ii) $d(xy) = xdy + ydx$, 任意 $x, y \in \overline{K}(E)$;

(iii) $da = 0$, 任一 $a \in \overline{K}$.

符号 dg 称为 E 上的微分, E 上的所有微分组成 $\overline{K}(E)$ 上的向量空间, 记为 Ω_E.

由上述定义, 对任一 $g(x,y) \in \overline{K}(E)$, 显然有

$$dg = \frac{\partial g}{\partial x}dx + \frac{\partial g}{\partial y}dy. \tag{3.17}$$

命题 3.4　Ω_E 是 $\overline{K}(E)$ 上的一维向量空间.

证明　$0 = df(x,y) = \frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy.$

因 $\frac{\partial f}{\partial y}=2y+a_1x+a_3\neq 0$(当 $\mathrm{char}\overline{K}=2$ 时, 可用 (3.8) 或 (3.9) 式代替 (3.2) 式). 故 $dy=-\frac{\partial f}{\partial x}/\frac{\partial f}{\partial y}\cdot dx$. 由 (3.17) 式可知 $\Omega_E=\overline{K}(E)dx$, 即证.

命题 3.5 设 $x\in\overline{K}(E)$, 则 dx 是 Ω_E 的 $\overline{K}(E)$ 基当且仅当 $\overline{K}(E)/\overline{K}(x)$ 是可分扩张.

证明见文献 [15], 第三章 §4, 定理 4 .

设 $\phi\colon E_1\to E_2$ 为有理映射, 它诱导映射

$$\begin{aligned}\phi^*:\quad &\Omega_{E_2}\longrightarrow\Omega_{E_1}\\ &gdx\longmapsto\phi^*(g)d\big(\phi^*(x)\big)\end{aligned}$$

$(g,x\in\overline{K}(E_2))$.

命题 3.6 设 $\phi\colon E_1\to E_2$ 为非常值有理映射, 则 ϕ 是可分的, 当且仅当

$$\phi^*:\quad \Omega_{E_2}\longrightarrow\Omega_{E_1}$$

是单射 (等价于非零).

证明 取 $y\in\Omega_{E_2}$, 使得 $\Omega_{E_2}=\overline{K}(E_2)dy$, 即 $\overline{K}(E_2)/\overline{K}(y)$ 是可分扩张, 因而 $\phi^*\overline{K}(E_2)/\phi^*\overline{K}(y)$ 也是可分的. 这时

$$\begin{aligned}\phi^*\text{是单射}\iff & d(\phi^*y)\neq 0\\ \iff & d(\phi^*y)\text{是}\Omega_{E_1}\text{的基 (命题 3.4)}\\ \iff & \overline{K}(E_1)/\overline{K}(\phi^*y)\text{是可分 (命题 3.5)}\\ \iff & \overline{K}(E_1)/\phi^*\overline{K}(E_2)\text{是可分的}.\end{aligned}$$

即证.

设点 $P\in E$, t_P 为 P 点的单值化子, 因 $\overline{K}(E)$ 是 $\overline{K}(t)$ 的可分扩张 (见文献 [12], 第二章命题 1.4), 故 dt_P 是 Ω_E 的基. 设 $\omega\in\Omega_E$, 则存在 $g\in\overline{K}(E)$, 使得 $\omega=gdt$. 定义微分 ω 在 P 的阶

$$\mathrm{ord}_P(\omega)=\mathrm{ord}_P(\omega/dt_P)=\mathrm{ord}_P(g).$$

上述定义不依赖于单值化子 t_P 的选择. 若 t'_P 为 P 的另一单值化子, 则 $(dt'_P/dt_P)(P)\neq 0$, 故

$$\mathrm{ord}_P\big(\omega/dt'_P\big)=\mathrm{ord}_P\big(\omega/dt_P\big)\mathrm{ord}_P\big(dt'_P/dt_P\big)=\mathrm{ord}_P\big(\omega/dt_P\big).$$

设非零微分 $\omega=gdx\in\Omega_{E_1}$, x 为 E 中点的 x 坐标, 即 $f(x,y)=0$, 易见最多存在 x 的 3 个值 a, 使得 $f(a,y)=0$ 有重根, 所以最多除 3 个点之外, $x-x(P)$ 是 P

点的单值化子, 从而 $\omega = gd(x - x(P))$, $\text{ord}_P(\omega) = \text{ord}_P(g)$, 可见对几乎所有的 P 有 $\text{ord}_P(\omega) = 0$. 定义微分 ω 决定的除子

$$\text{div}(\omega) = \sum_P \text{ord}_P(\omega)(P),$$

上式右端是一个有限和.

设 ω_1 和 ω_2 为两个非零除子, 则存在 $g \in \Omega_E$, 使得 $\omega_1 = g\omega_2$, 从而 $\text{div}(\omega_1) = \text{div}(g) + \text{div}(\omega_2)$, 即任一非零微分的除子都是线性等价的. 该等价类就是典范除子类 (见 (3.15) 式).

E 上的微分 $\omega = dx/(2y + a_1x + a_3)$ 称为不变微分, 该名称的由来是因为有

命题 3.7 ω 如上定义, 则对任一点 $Q \in E$, 有

$$\tau_Q^*(\omega) = \omega,$$

其中 $\tau_Q(P) = P + Q$, $\forall P \in E$.

证明 见文献 [12], 第三章命题 5.1.

命题 3.8 设 ω 为 E 的不变微分, $\phi, \psi: E' \to E$ 为两个同种映射, 则

$$(\phi + \psi)^*(\omega) = \phi^*(\omega) + \psi^*(\omega).$$

证明 见文献 [12], 第三章定理 5.2.

命题 3.9 设 $K \in \mathbb{F}_q$, K 的特征为 p, E 为定义在 K 上的椭圆曲线, ϕ_q 为 E 上的 q 阶 Frobenius 映射. m, n 为整数, 则有

$$m + n\phi_q: \quad E \longrightarrow E$$

为可分当且仅当 $p \nmid m$. 特别地, $1 - \phi_q$ 是可分的.

证明 设 ω 为 E 的不变微分, 则 $m + n\phi_q$ 为可分, 当且仅当 $(m + n\phi_q)^*(\omega) \neq 0$(命题 3.6).

由于 $[m+1]^*\omega = [m]^*\omega + \omega$(命题 3.8), 显然 $[1]^*\omega = \omega$, 利用归纳法可以证明 $[m]^*\omega = m\omega$.

易见, 对任一微分 dg, 有 $\phi_q^*(dg) = d(\phi_q^* g) = d(g^q) = 0$, 所以 $(m + n\phi_q)^*\omega = [m]^*\omega = m\omega$, 当且仅当 $p|m$ 时, $m\omega = 0$, 证毕.

同种的对偶

对任一 $\phi \in \text{Hom}(E_1, E_2)$, 存在一个从 E_2 到 E_1 的映射

$$E_2 \xrightarrow{\kappa_2} \text{Pic}^\circ(E_2) \xrightarrow{\phi^*} \text{Pic}^\circ(E_1) \xrightarrow{\kappa_1^{-1}} E_1,$$

它将 $Q \in E_2$ 映射为

$$\begin{aligned}
\kappa_1^{-1}\phi^*\kappa_2(Q) &= \kappa_1^{-1}\phi^*\big((Q)-(\mathcal{O})\big)\\
&= \kappa_1^{-1}\Big(\sum_{P\in\phi^{-1}(Q)} e_\phi(P)(P) - \sum_{T\in\phi^{-1}(\mathcal{O})} e_\phi(T)(T)\Big)\\
&= \sum_{P\in\phi^{-1}(Q)} [e_\phi(P)]P - \sum_{T\in\phi^{-1}(\mathcal{O})} [e_\phi(T)]T \qquad (3.18)\\
&= [\deg_i\phi]\Big(\sum_{T\in\phi^{-1}(\mathcal{O})} (P+T) - \sum_{T\in\phi^{-1}(\mathcal{O})} T\Big)\\
&= [\deg_i\phi]\cdot[\deg_s\phi]\cdot P = [\deg\phi]P,
\end{aligned}$$

其中 P 可为 $\phi^{-1}(Q)$ 中任一点, 这里利用了定理 3.8. 易见 $\widehat{\phi}(\mathcal{O}) = \mathcal{O}$, 将上述映射记为 $\widehat{\phi}$, 称它为 ϕ 的对偶, 以下将证明 $\widehat{\phi}$ 是一个同种映射. 由 (3.18) 式可知

$$\widehat{\phi}\phi = [\deg\phi]. \qquad (3.19)$$

定理 3.11 设 $\phi:\ E_1 \to E_2$ 为次数 m 的非常值的同种映射, 则存在惟一的同种映射

$$\widehat{\phi}:\quad E_2 \longrightarrow E_1,$$

使得

$$\widehat{\phi}\cdot\phi = [m].$$

证明 首先证明惟一性. 若 $\widehat{\phi}$ 和 $\widehat{\phi}'$ 都具有上述性质, 则

$$\big(\widehat{\phi}-\widehat{\phi}'\big)\cdot\phi = [m]-[m] = [0],$$

故 $\widehat{\phi}-\widehat{\phi}'$ 是恒等映射, 亦即 $\widehat{\phi}=\widehat{\phi}'$.

今证 $\widehat{\phi}$ 的存在性. 设 $\psi:\ E_2 \to E_3$ 为次数 n 的非常值的同种映射, 则

$$\big(\widehat{\phi}\cdot\widehat{\psi}\big)\cdot(\psi\cdot\phi) = \widehat{\phi}\cdot\big(\widehat{\psi}\psi\big)\cdot\phi = [n]\widehat{\phi}\cdot\phi = [mn].$$

可见 $\widehat{\phi}\cdot\widehat{\psi}$ 即为 $\widehat{\psi\cdot\phi}$, 我们若能构造 $\widehat{\phi}$, $\widehat{\psi}$, 即能构造 $\widehat{\psi\cdot\phi}$.

存在域 F, 使得 $\phi^*\big(\overline{K}(E_2)\big) \subset F \subset \overline{K}(E_1)$ 且 $\overline{K}(E_1)/F$ 为纯不可分扩张, $F/\phi^*\big(\overline{K}(E_2)\big)$ 为可分扩张. 设 $q=\deg_i(\phi) = [\overline{K}(E_1):F]$, q 阶 Frobenius 映射 $\psi:\ E_1 \to E_1^q$. 由于 $q=\deg\psi = [\overline{K}(E_1):\psi^*\overline{K}(E_1^q)]$, 可见 $F=\psi^*\big(\overline{K}(E_1^q)\big)$. 由命题 3.2, 存在可分同种映射 $\lambda:\ E_1^q \to E_2$, 使得 $\psi^*\cdot\lambda^*\big(\overline{K}(E_2)\big) = \phi^*\big(\overline{K}(E_2)\big)$, 即 $\phi = \lambda\cdot\psi$.

利用上述结论, 我们仅需证明当 ϕ 为可分同种映射或 Frobenius 映射时, 存在同种映射 $\widehat{\phi}$ 即可.

情形 1: 设 ϕ 是可分的, 这时

$$\#\mathrm{Ker}\phi = \deg\phi = m \quad (\text{定理 } 3.8),$$

则有 $\mathrm{Ker}\phi \subset \mathrm{Ker}[m]$. 在定理 3.10 中, 取 $\phi: E_1 \to E_2$, $[m]: E_1 \to E_1$, 可知存在 $\widehat{\phi}: E_2 \to E_1$, 使得 $\widehat{\phi}\phi = [m]$.

情形 2: 设 ϕ 是 $q = p^e$ 阶 Frobenius 映射, 令 ϕ_p 为 p 阶 Frobenius 映射, 因 $\phi = \phi_p^e$, 仅需证明存在同种映射 $\widehat{\phi}_p$ 即可. 由于 $[p]$ 是不可分的 (命题 3.9), 它可表示为 $[p] = \psi\phi_p^r$, 其中 ψ 为可分映射, $r \geqslant 1$, 可见 $\widehat{\phi}_p = \psi\phi_p^{r-1}$. 证毕.

由定理 3.11 及 (3.18) 式可知 $\kappa_1^{-1}\phi^*\kappa_2$ 是同种映射, 它就是 $\widehat{\phi}$.

定理 3.12　对任一整数 m, 有 $\widehat{[m]} = [m]$ 及 $\deg[m] = m^2$, 所以当 $\mathrm{char}(K) = 0$ 或 $\mathrm{char}(K)$ 与 m 互素时, $[m]$ 是可分的.

证明　设 $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, 则 $\widehat{\phi+\psi} = \widehat{\phi} + \widehat{\psi}$ (见文献 [12], 第三章定理 6.2). 当 $m = 0$ 或 ± 1 时, 定理显然成立. 由于 $\widehat{[m \pm 1]} = \widehat{[m]} \pm \widehat{[1]}$, 利用归纳法, 可知第 1 个结论成立. 令 $d = \deg[m]$, 由 (3.19) 式, $[d] = \widehat{[m]} \cdot [m] = [m^2]$, 因而, $[d - m^2] = 0$, 所以 $d = m^2$. 后一结论来自命题 3.9, 证毕.

定理 3.13　设 $\phi \in \mathrm{Hom}(E_1, E_2)$, $\psi \in \mathrm{Hom}(E_2, E_3)$, 则

(1) $\deg\phi = \deg\widehat{\phi}$;

(2) $\phi\widehat{\phi} = [\deg\phi]$;

(3) $\widehat{\widehat{\phi}} = \phi$;

(4) $\widehat{\psi\phi} = \widehat{\phi}\widehat{\psi}$.

证明

(1) 记 $d = \deg\phi$, 由定理 3.12, $d^2 = \deg[d] = \deg(\widehat{\phi}\phi) = \deg\widehat{\phi} \cdot \deg\phi = d \cdot \deg\widehat{\phi}$, 故 $\deg\widehat{\phi} = d$.

(2) $(\phi\widehat{\phi})\phi = \phi(\widehat{\phi}\phi) = \phi \cdot [d] = [d] \cdot \phi$, 故 $\phi\widehat{\phi} = [d]$.

(3) $[d]\widehat{\widehat{\phi}} = (\phi\widehat{\phi})\widehat{\widehat{\phi}} = \phi(\widehat{\widehat{\phi}\phi}) = \phi[\deg\widehat{\phi}] = [d]\phi$, 故 $\widehat{\widehat{\phi}} = \phi$.

(4) $\psi\phi \cdot \widehat{\phi}\widehat{\psi} = [\deg\ \phi] \cdot \psi\widehat{\psi} = [\deg\phi \cdot \deg\psi] = [\deg\phi\psi] = \psi\phi \cdot \widehat{\psi\phi}$, 故 $\widehat{\psi\phi} = \widehat{\phi}\widehat{\psi}$.

证毕.

例 3.1　设 K 是特征不等于 2 的域, 而 $a, b \in K$ 且 $b \neq 0, r := a^2 - 4b \neq 0$. 考虑下面两条椭圆曲线:

$$E_1: \quad y^2 = x^3 + ax^2 + bx,$$

$$E_2: \quad Y^2 = X^3 - 2aX^2 + rX.$$

令

$$\begin{aligned}\phi: \quad & E_1 \longrightarrow E_2, \\ & (x,y) \longmapsto \Big(\frac{y^2}{x^2}, \frac{y(b-x^2)}{x^2}\Big),\end{aligned}$$

则 ϕ 是一个同种映射, 其对偶为

$$\begin{aligned}\widehat{\phi}: \quad & E_2 \longrightarrow E_1, \\ & (X,Y) \longmapsto \Big(\frac{Y^2}{4X^2}, \frac{Y(r-X^2)}{8X^2}\Big),\end{aligned}$$

且它在不变微分上的作用为

$$\phi^*\Big(\frac{dX}{2Y}\Big) = -\frac{dx}{2y}.$$

证明 直接验证, 可知 ϕ 是一个同种映射, 又显然 ϕ 的次数是 2, 再直接验证可知, 在 E_2 上有 $\phi\circ\widehat{\phi} = [2]_{E_2}$, 而在 E_1 上有 $\widehat{\phi}\circ\phi = [2]_{E_1}$, 于是由定理 3.14 知 $\widehat{\phi}$ 是 ϕ 的对偶同种. 下面证明关于不变微分的结论. 由定义, 有

$$\phi(x) = \frac{y^2}{x^2}, \quad \phi(y) = \frac{y(b-x^2)}{x^2},$$

因此

$$\phi^*\Big(\frac{dX}{Y}\Big) = \frac{d\phi(x)}{\phi(y)} = \frac{\phi'(x)dx}{\phi(y)}.$$

但是, $y^2 = x^3 + ax^2 + bx$ 意味着 $2yy' = 3x^2 + 2ax + b$, 因此

$$\begin{aligned}\phi'(x) &= \frac{d}{dx}\Big(\frac{y^2}{x^2}\Big) = \frac{2yy'x - 2y^2}{x^3} \\ &= \frac{(3x^2+2ax+b)x - 2(x^3+ax^2+bx)}{x^3} \\ &= \frac{x^2-b}{x^2}.\end{aligned}$$

所以

$$\phi^*\Big(\frac{dX}{Y}\Big) = \frac{\frac{x^2-b}{x^2}dx}{\frac{y(b-x^2)}{x^2}} = -\frac{dx}{y}.$$

证毕.

§3.4 Tate 模和 Weil 对

设 E/K 为椭圆曲线, m 为正整数, 定义

$$E[m] = \{P \in E(\overline{K}) | [m]P = \mathcal{O}\},$$

即 $E[m]=\mathrm{Ker}[m]$.

定理 3.14　(1) 若 $\mathrm{char}(K)=0$ 或 $m\geqslant 2$ 与 $\mathrm{char}(K)$ 互素, 则

$$E[m]=(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z});$$

(2) 当 $\mathrm{char}(K)=p>0$ 时,

$$E[p^e]=\{\mathcal{O}\},\quad e=1,2,3,\cdots,$$

或

$$E[p^e]=\mathbb{Z}/p^e\mathbb{Z},\quad e=1,2,3,\cdots.$$

证明　当 $\mathrm{char}(K)=0$ 或 $m\geqslant 2$ 与 $\mathrm{char}(K)$ 互素时, $[m]$ 是可分的 (定理 3.12), 从而 $\#E[m]=\deg[m]=m^2$(定理 3.8). 对 m 的任一因子 d, 也可类似得到 $\#E[d]=d^2$. 利用 Abel 群的基本定理, 将 $E[m]$ 表为循环群的直积时, 仅可能有 $E[m]=(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$.

当 $\mathrm{char}(K)=p>0$ 时, 以 ϕ_p 表示 Frobenius 变换, 它是纯不可分的 (定理 3.7), 我们有

$$\#E[p^e]=\deg_s[p^e]=\deg_s^e\left(\widehat{\phi_p}\phi_p\right)=\left(\deg_s\widehat{\phi_p}\right)^e,$$

因 $\deg\widehat{\phi_p}=\deg\phi_p=p$(定理 3.13), 故 $\deg_s\widehat{\phi_p}=1$ 或 p.

当 $\deg_s\widehat{\phi_p}=1$ 时, 对所有的 e 有 $\#E[p^e]=1$. 当 $\deg_s\widehat{\phi_p}=p$ 时, 对所有的 e 有 $\#E[p^e]=p^e$, 从而 $E[p^e]=\mathbb{Z}/p^e\mathbb{Z}$, 证毕.

当 $\#E(p^e)=1$(任一 $e\geqslant 1$) 时, E 称为超奇异椭圆曲线.

设 l 为素数, 相对于映射

$$E[l^{n+1}]\xrightarrow{[l]}E[l^n]$$

的反向极限群

$$T_l(E)=\varprojlim_n E[l^n],$$

称为 E 的 (l-adic)Tate 模. $T_l(E)$ 中任一元素可表为

$$\alpha=(\alpha_1,\alpha_2,\cdots,),$$

其中 $\alpha_i\in E[l^i]$, 且 $[l]\alpha_{i+1}=\alpha_i\ (i=1,2,\cdots)$. 因 $E[l^i]$ 是 $\mathbb{Z}/l^i\mathbb{Z}$ 上的模, 故 $T_l(E)$ 是 l-adic 整数环 $\mathbb{Z}_l$ 上的模. 取 $u=\sum_{i=0}^{\infty}a_il^i\in\mathbb{Z}_l$, 则

$$u\cdot\alpha=(u\alpha_1,u\alpha_2,\cdots)=(a_0\alpha_1,(a_0+a_1l)\alpha_2,\cdots)\in T_l(E).$$

由定理 3.14 可知, 当 $l \neq \mathrm{char}(K)$ 时, $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$; 当 $l = \mathrm{char}(K)$ 时, $T_l(E) \cong \{0\}$ 或 $\mathbb{Z}_l$.

设 $\mathrm{char}(K) = 0$ 或 $m \geqslant 2$ 且与 $\mathrm{char}(K)$ 互素, $T \in E[m]$, 则存在 $f \in \overline{K}(E)$, 使得 $\mathrm{div}(f) = m(T) - m(\mathcal{O})$ (推论 3.1), 取 $T' \in E(\overline{K})$, 使得 $[m](T') = T$, 同样存在 $g \in \overline{K}(E)$, 使得

$$\mathrm{div}(g) = [m]^*(T) - [m]^*(\mathcal{O}) = \sum_{R \in E[m]} (T' + R) - (R),$$

易见 $f \cdot [m]$ 与 g^m 具有相同的除子, 它们仅差 $\overline{K}^*$ 中一个常数因子, 可以假设 $f \cdot [m] = g^m$.

设 $S \in E[m]$ (S 与 T 可以相同), 对任一 $X \in E$,

$$g(X + S)^m = f([m]X + [m]S) = f([m]X) = g(X)^m,$$

故 $e_m(S, T) = g(X + S)/g(X)$ 是一个 m 次单位根 ($\overline{K}(E)$ 中的任一函数或常数, 或取遍 $\overline{K} \cup \{\infty\}$ 所有的值, 所以 $e_m(S, T)$ 是一个常数). g 的取法可以差一个常数因子, 但这不影响 $e_m(S, T)$ 的值, 故得到

$$e_m: \quad E[m] \times E[m] \longrightarrow \mu_m,$$

μ_m 为 m 次单位根组成的群, e_m 称为 Weil 对.

Weil 对还有一个等价的定义, 它更便于计算. 设 $S, T \in E[m]$, 取除子 D_S 和 D_T, 使得 $D_S \sim (S) - (\mathcal{O}), D_T \sim (T) - (\mathcal{O})$, 且 D_S 与 D_T 的表达式中不出现公共的支撑 (例如取 $D_S = ([k+1]S) - ([k]S)$, 使得 $[k+1]S, [k]S, T, \mathcal{O}$ 互不相同), 存在 $f_S, f_T \in \overline{K}(E)$, 使得 $\mathrm{div}(f_S) = mD_S, \mathrm{div}(f_T) = mD_T$. 若 $f \in \overline{K}(E), \mathrm{div}(f)$ 与除子 $D = \sum n_P(P)$ 没有公共支撑, 则定义 $f(D) = \prod f(P)^{n_P}$, 故有

$$e_m(S, T) = f_S(D_T)/f_T(D_S). \tag{3.20}$$

上式的证明见 (文献 [12], 第三章习题 3.16).

定理 3.15 Weil对具有下述性质(设 $S, S_1, S_2, T, T_1, T_2 \in E[m]$):

(1) 双线性:

$$e_m(S_1 + S_2, T) = e_m(S_1, T)e_m(S_2, T),$$
$$e_m(S, T_1 + T_2) = e_m(S, T_1)e_m(S, T_2);$$

(2) 交错性:

$$e_m(S, T) = e_m(T, S)^{-1};$$

(3) 非退化：若对任一 $S \in E[m]$, 有 $e_m(S,T)=1$, 则 $T=\mathcal{O}$;

(4) 对任一 $\delta \in G_{\overline{K}/K}$, 有 $e_m(S,T)^\delta = e_m(S^\delta, T^\delta)$;

(5) 若 $S \in E[mm']$, $T \in E[m]$, 则 $e_{mm'}(S,T) = e_m([m']S,T)$.

证明　(1) 因

$$e_m(S_1+S_2,T) = \frac{g(X+S_1+S_2)}{g(X)} = \frac{g(X+S_1+S_2)}{g(X+S_1)} \cdot \frac{g(X+S_1)}{g(X)}$$
$$= e_m(S_2,T)e_m(S_1,T),$$

故第一式成立. 假设对 T_1, T_2, T_1+T_2 如上述分别构造了函数 f_1, f_2, f_3, g_1, g_2, g_3, 取 $h \in \overline{K}(E)$, 使得

$$\operatorname{div}(h) = (T_1+T_2) - (T_1) - (T_2) + (\mathcal{O}),$$

则 $\operatorname{div}(f_3/f_1f_2) = m \ \operatorname{div}(h)$, 即 $f_3 = cf_1f_2h^m$, c 为 $\overline{K}^*$ 中一常数. 利用 $f_i \cdot [m] = g_i^m$, 并开 m 次方得 $g_3 = c'g_1g_2(h\cdot[m])$, c' 为一常数, 从而

$$e_m(S,T_1+T_2) = \frac{g_3(X+S)}{g_3(X)} = \frac{g_1(X+S)g_2(X+S)h([m]X+[m]S)}{g_1(X)g_2(X)h([m]X)}$$
$$= e_m(S,T_1) \ \ e_m(S,T_2).$$

(2) 由 (1),

$$e_m(S+T,S+T) = e_m(T,T)e_m(T,S)e_m(S,T)e_m(S,S),$$

仅需要证明对任一 $T \in E[m]$ 有 $e_m(T,T)=1$. 以 τ_T 表示平移变换 $P \mapsto P+T$, 如上述构造 f 与 g, 由于

$$\operatorname{div}\left(\prod_{i=0}^{m-1} f \circ \tau_{[i]T}\right) = m\left\{\sum_{i=0}^{m-1}([1-i]T) - \sum_{i=0}^{m-1}([-i]T)\right\} = 0,$$

故 $\prod_{i=0}^{m-1} f \circ \tau_{[i]T}$ 是一个常数. 取 T', 使得 $[m]T' = T$, 由于

$$g(X+[i]T')^m = f([m]X+[mi]T') = f([m]X+[i]T),$$

故 $\prod_{i=0}^{m-1} g \circ \tau_{[i]T'}$ 也是常数, 它在 X 与 $X+T'$ 上取相同的值, 即

$$\prod_{i=0}^{m-1} g(X+[i]T') = \prod_{i=0}^{m-1} g(X+[1+i]T'),$$

由此推出 $g(X) = g(X+T)$. 所以 $e_m(T,T) = \frac{g(X+T)}{g(X)} = 1$.

(3) 若对所有的 $S\in E[m]$ 有 $e_m(S,T)=1$, 则对所有的 $S\in E[m]$ 有 $g(X+S)=g(X)$, 即 g 在 τ_S^* 作用下不变. $[m]$ 是可分的, 所以 $\mathrm{Gal}(\overline{K}(E)/[m]^*\overline{K}(E))\cong\{\tau_S^*|S\in E[m]\}$(定理 3.8), 因而 $g\in[m]^*\overline{K}(E)$, 存在 $h\in\overline{K}(E)$, 使得 $g=h\cdot[m]$. 由于 $(h\cdot[m])^m=g^m=f\cdot[m]$, 可见 $f=ch^m\quad(c\in\overline{K}^*)$, 从而

$$m\ \operatorname{div}(h)=\operatorname{div}(f)=m(T)-m(\mathcal{O}),$$

可见 $\operatorname{div}(h)=(T)-(\mathcal{O})$, 左端为主除子, 故 $T=\mathcal{O}$(推论 3.1).

(4) 设 $\delta\in G_{\overline{K}/K}$, f 和 g 为上述对应 T 构造的函数, 则对应 T^δ 构造的函数为 f^δ 和 g^δ (f^δ 表示将 δ 作用到有理函数 f 的所有系数上所得到的函数), 我们有

$$e_m(S^\delta,T^\delta)=\frac{g^\delta(X+S^\delta)}{g^\delta(X)}=\Big(\frac{g(X+S)}{g(X)}\Big)^\delta=e_m(S,T)^\delta.$$

(5) 我们有 $\operatorname{div}(f^{m'})=m'm(T)-m'm(\mathcal{O})$ 及

$$(g\circ[m'])^{mm'}=(f\circ[mm'])^{m'}=f^{m'}\circ[mm'],$$

故

$$e_{mm'}(S,T)=\frac{g\circ[m'](X+S)}{g\circ[m'](X)}=\frac{g([m']X+[m']S)}{g([m']X)}=e_m([m']S,T).$$

证毕.

定理 3.16 *存在 $S,T\in E[m]$, 使得 $e_m(S,T)$ 为 m 次本原单位根. 特别地, 当 $E[m]\subset E(K)$ 时, 有 $\mu_m\subset K$.*

证明 若存在 m 的真因子 d, 使得 $e_m(S,T)^d=1\quad(\forall S,T\in E[m])$, 由于 $e_m(S,T)^d=e_m([d]S,T)=1$ 对所有的 $T\in E[m]$ 成立, 所以 $[d]S=\mathcal{O}$(定理 3.15 (3)), S 为 $E[m]$ 中任一点, 这不可能.

当 $E[m]\subset E(K)$ 时, $e_m(S,T)$ 在 $G_{\overline{K}/K}$ 作用下固定不变 (定理 3.15 (4)), 故 $e_m(S,T)\in K$, 即 $\mu_m\subset K$, 证毕.

定理 3.17 设 $\phi\in\mathrm{Hom}(E_1,E_2)$, $S\in E_1[m],T\in E_2[m]$, 则

$$e_m(\phi(S),T)=e_m(S,\widehat{\phi}(T)).$$

证明 对于 T, 如上构造函数 f 和 g, 由于 $\kappa_1(\widehat{\phi}(T))=\phi^*((T))-\phi^*((\mathcal{O}))$, 即 $\widehat{\phi}(T)$ 是除子 $\phi^*((T))-\phi^*((\mathcal{O}))$ 中出现的所有点 (在 E_1 上) 之和. 利用推论 3.1, 存在 $h\in\overline{K}(E_1)$, 使得

$$\phi^*((T))-\phi^*((\mathcal{O}))=\big(\widehat{\phi}(T)\big)-(\mathcal{O})+\operatorname{div}(h).$$

上式左端乘 m 即为 $\operatorname{div}(f\circ\phi)$(文献 [12], 命题 2.3 (b)), 故

$$\operatorname{div}\left(\frac{f\circ\phi}{h^m}\right)=m(\widehat{\phi}(T))-m(\mathcal{O}),$$

而

$$\frac{f\circ\phi}{h^m}\circ[m]=\frac{f\circ[m]\circ\phi}{h^m\circ[m]}=\left(\frac{g\circ\phi}{h\circ[m]}\right)^m,$$

因此

$$\begin{aligned}e_m(S,\widehat{\phi}(T))&=\frac{(g\circ\phi/h\circ[m])(X+S)}{(g\circ\phi/h\circ[m])(X)}\\&=\frac{g(\phi(X)+\phi(S))h([m]X)}{g(\phi(X))\cdot h([m]X+[m]S)}=e_m(\phi(S),T).\end{aligned}$$

证毕.

设 l 为异于 $\operatorname{char}(K)$ 的素数, 将 $E[l^n]$ $(n=1,2,\cdots)$ 上的 Weil 对合并在一起可以得到 Tate 模 $T_l(E)$ 上的 (l-adic)Weil 对. 对应 l 次升幂映射

$$\mu_{l^{n+1}}\xrightarrow{\ l\ }\mu_{l^n}.$$

定义反向极限群

$$T_l(\mu)=\varprojlim_n\mu_{l^n}.$$

设 $a=\sum_{i=0}^{\infty}a_il^i\in\mathbb{Z}_l$, $\Lambda=(\lambda_1,\lambda_2,\cdots)\in T_l(\mu)$, 定义

$$a\Lambda=(\lambda_1^a,\lambda_2^a,\cdots)=(\lambda_1^{a_0},\lambda_2^{a_0+a_1l},\cdots),$$

$T_l(\mu)$ 可看作 $\mathbb{Z}_l$ 上的模.

设 $S=(S_1,S_2,\cdots)\in T_l(E)$, $T=(T_1,T_2,\cdots)\in T_l(E)$, 其中 S_n 和 T_n 属于 $E[l^n]$. 令

$$e(S,T)=(e_l(S_1,T_1),e_{l^2}(S_2,T_2),\cdots),$$

由于

$$\begin{aligned}e_{l^{n+1}}(S_{n+1},T_{n+1})^l&=e_{l^{n+1}}(S_{n+1},[l]T_{n+1})\\&=e_{l^n}([l]S_{n+1},T_n)=e_{l^n}(S_n,T_n)\end{aligned}$$

(定理 3.15 的 (1) 和 (5)), 可见 $e(S,T)\in T_l(\mu)$, 从而得到 Tate 模上的 Weil 对

$$e:\quad T_l(E)\times T_l(E)\longrightarrow T_l(\mu),$$

由定理 3.15, 易证 e 也具有双线性、交错性、非退化性. 同样, 若 $\phi \in \mathrm{Hom}(E_1, E_2)$, $S \in T_l(E_1)$, $T \in T_l(E_2)$, 则

$$e(\phi(S), T) = e(S, \widehat{\phi}(T)),$$

这里 $\phi(S) = (\phi(S_1), \ \phi(S_2), \cdots)$.

§3.5 有限域上的椭圆曲线

设 $K = \mathbb{F}_q$(包含 q 个元素的有限域), E/K 为定义在有限域上的椭圆曲线. 令

$$E(K) = \{(x, y) \in E | x, y \in K\} \bigcup \{\mathcal{O}\},$$

$E(K)$ 称为 E 的 K 有理点集合, 它是一个有限集. 计算 $\#E(K)$ 是研究定义在有限域上的椭圆曲线的核心问题.

在方程 (3.2) 中, 当 x 取遍 K 的元素时, 约有一半的情形使 (3.2) 式左端的 2 次方程有 2 个解, 所以 $\#E(K)$ 大致为 $q+1$. E.Artin 在他的博士论文中猜想有下述定理 3.18, 后来 Hasse 给出了证明.

定理 3.18 设 $K = \mathbb{F}_q$, E/K 为椭圆曲线, 则

$$|\#E(K) - q - 1| \leqslant 2\sqrt{q}.$$

证明 在 $E(\overline{K})$ 上定义 q 阶 Frobenius 变换

$$\begin{aligned} \phi: \quad & E \longrightarrow E \\ & (x, y) \longmapsto (x^q, y^q), \end{aligned}$$

且 $\phi(\mathcal{O}) = \mathcal{O}$. 当且仅当 $\phi(P) = P$ 时, $P \in E(K)$, 所以 $E(K) = \mathrm{Ker}(1 - \phi)$. 由于 $1 - \phi$ 是可分的 (命题 3.9), 因而 $\#E(K) = \deg(1 - \phi)$(定理 3.10), 利用下述引理 3.4 可证得本定理.

设 A 为交换群, 函数

$$d: \quad A \longrightarrow \mathbb{R} \ (\text{实数域})$$

称为二次型, 如果

(1) 对任意 $\alpha \in A$, $d(-\alpha) = d(\alpha)$;

(2) 令

$$\begin{aligned} & A \times A \longrightarrow \mathbb{R} \\ & (\alpha, \beta) \longmapsto d(\alpha + \beta) - d(\alpha) - d(\beta), \end{aligned}$$

(α, β) 具有双线性.

一个二次型称为正定的, 如果

(3) 对任一 $\alpha \in A$, $d(\alpha) \geqslant 0$;

(4) 当且仅当 $\alpha = 0$ 时, $d(\alpha) = 0$.

引理 3.3 设 E_1 和 E_2 为定义在同一域上的椭圆曲线, 则映射

$$\deg: \quad \operatorname{Hom}(E_1, E_2) \longrightarrow \mathbb{Z}$$

是正定二次型.

证明 仅需证明若 $\phi, \psi \in \operatorname{Hom}(E_1, E_2)$, 则

$$\langle \phi, \psi \rangle = \deg(\phi + \psi) - \deg \phi - \deg \psi$$

具有双线性, 其他条件显然符合. 利用 (3.19) 式, 有

$$\begin{aligned}[\langle \phi, \psi \rangle] &= [\deg(\phi + \psi)] - [\deg \phi] - [\deg \psi] \\ &= (\widehat{\phi + \psi})(\phi + \psi) - \widehat{\phi}\phi - \widehat{\psi}\psi = \widehat{\phi}\psi + \widehat{\psi}\phi.\end{aligned}$$

易见双线性成立, 证毕.

引理 3.4 设 A 为交换群, $d: A \longrightarrow \mathbb{Z}$ 为正定二次型, 则对所有 ϕ, $\psi \in A$ 有

$$|d(\phi - \psi) - d(\phi) - d(\psi)| \leqslant 2\sqrt{d(\phi)d(\psi)}.$$

证明 令 $L(\phi, \psi) = d(\phi - \psi) - d(\phi) - d(\psi)$, L 具有双线性. 由于

$$\begin{aligned}-2(m+1)d(\phi) &= (m+1)L\big(\phi, \phi\big) = L\big((m+1)\phi, \phi\big) \\ &= d(m\phi) - d\big((m+1)\phi\big) - d(\phi),\end{aligned}$$

故 $d\big((m+1)\phi\big) = d(m\phi) + (2m+1)d(\phi)$, 利用归纳法易证 $d(m\phi) = m^2 d(\phi)$. 任取 $m, n \in \mathbb{Z}$, $mnL(\phi, \psi) = L(m\phi, n\psi) = d(m\phi - n\psi) - m^2 d(\phi) - n^2 d(\psi)$, 由于 d 是正定的, 故

$$0 \leqslant d(m\phi - n\psi) = m^2 d(\phi) + mnL(\phi, \psi) + n^2 d(\psi),$$

因而 $L^2(\phi, \psi) \leqslant 4d(\phi)d(\psi)$, 即得引理, 证毕.

在引理 3.4 中取 $A = \operatorname{End}(E)$, ϕ 为 q 阶 Frobenius 变换, $\psi = 1$, 由于 $\deg(1-\phi) = \#E(K)$, $\deg \phi = q$, $\deg \psi = 1$, 由此可证明定理 3.18.

设 $\psi \in \operatorname{End}(E)$, 素数 l 与 q 互素. ψ 与 $[l^n]$ 可交换, 所以 $\psi(E[l^n]) \subset E[l^n]$, ψ 可诱导 Tate 模 $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ 上的一个线性变换 ψ_l. 当 $T_l(E)$ 取定一组 $\mathbb{Z}_l$ 基后, ψ_l 可用 $\mathbb{Z}_l$ 上的一个 2 阶方阵表示, 因而相应可计算 $\det \psi_l$ 和 $\operatorname{tr}(\psi_l)$.

定理 3.19 设 $\psi \in \mathrm{End}(E)$, 则

$$\det(\psi_l) = \deg\psi, \qquad \mathrm{tr}(\psi_l) = 1 + \deg\psi - \deg(1-\psi).$$

可见, $\det(\psi_l)$ 和 $\mathrm{tr}(\psi_l)$ 都是整数, 且不依赖于 l.

证明 取 v_1 和 v_2 为 $T_l(E)$ 的 $\mathbb{Z}_l$ 基, 在这组基上,

$$\psi_l = \begin{pmatrix} a & b \\ c & d \end{pmatrix}, \qquad a,b,c,d \in \mathbb{Z}_l.$$

设 e 为 $T_l(E)$ 上的 Weil 对, 我们有

$$\begin{aligned} e(v_1,v_2)^{\deg\psi} &= e([\deg\psi]v_1, v_2) = e(\widehat{\psi}\psi v_1, v_2) \\ &= e(\psi v_1, \psi v_2) = e(av_1 + cv_2, bv_1 + dv_2) \\ &= e(v_1,v_2)^{ad-bc} = e(v_1,v_2)^{\det(\psi_l)}, \end{aligned}$$

这里利用了 $e(v_1,v_1) = e(v_2,v_2) = 1$, $e(v_2,v_1) = e(v_1,v_2)^{-1}$. 由于 e 是非退化的, 故得 $\det(\psi_l) = \deg\psi$. 对于任意 2 阶方阵 A 都有

$$\det(1-A) = 1 + \det A - \mathrm{tr}(A).$$

于是得到 $\mathrm{tr}(\psi_l)$ 的表达式, 证毕.

设 ϕ 为 q 阶 Frobenius 变换, 可见 ϕ_l 的特征多项式为

$$\det(T-\phi_l) = T^2 - \mathrm{tr}(\phi_l)T + \deg\phi = T^2 - tT + q,$$

其中 t 为不依赖于 l 的整数, 称为 ϕ 的迹. 由于 $\phi_l^2 - t\phi_l + q = 0$, 这表示 $\phi^2 - t\phi + q$ 在 $E[l^n]$ $(n = 1,2,\cdots)$ 上的作用恒为 $\mathcal{O}$, 因而它在 E 上的作用恒为 $\mathcal{O}$, 即 $\phi^2 - t\phi + q = 0$, ϕ 适合 2 次方程 $x^2 - tx + q = 0$. 利用定理 3.19 的第 2 个恒等式 (取 $\psi = \phi$),

$$\#E(K) = \deg(1-\phi) = 1 + q - t \tag{3.21}$$

因而 $|t| \leqslant 2\sqrt{q}$(定理 3.18), 二项式 $x^2 - tx + q$ 有 2 个根 α 和 β(在复数域中), 且 $|\alpha| = |\beta| = \sqrt{q}$, α 和 β 就是 ϕ_l 的特征根, ϕ_l^n 的特征根就是 α^n 和 β^n. 记 $K_n = \mathbb{F}_{q^n}$, ϕ^n 为 q^n 阶 Frobenius 变换, 因而

$$\begin{aligned} \#E(K_n) &= \mathrm{Ker}(1-\phi^n) = \deg(1-\phi^n) = \det(1-\phi_l^n) \\ &= 1 + \det(\phi_l^n) - \mathrm{tr}(\phi_l^n) = 1 + q - \alpha^n - \beta^n. \end{aligned} \tag{3.22}$$

令 $V_0 = 2, V_1 = t = \alpha + \beta, V_n = tV_{n-1} - qV_{n-2} \ (n \geqslant 2)$, 易见 $V_n = \alpha^n + \beta^n$. 利用这个递推公式可以方便地计算 V_n. 最初的几个 V_n 为

$$\begin{aligned} V_2 &= t^2 - 2q, \\ V_3 &= t^3 - 3tq, \\ V_4 &= t^4 - 4t^2q + 2q^2, \\ V_5 &= t^5 - 5t^3q + 5tq^2, \\ V_6 &= t^6 - 6t^4q + 9t^2q^2 - 2q^3, \\ V_7 &= t^9 - 7t^5q + 14t^3q - 7tq^3. \end{aligned} \tag{3.23}$$

§3.6 p 挠元点和自同态环

在这一节, 我们将刻画一下特征 $p > 0$ 的域上椭圆曲线的 p 挠元 (torsion) 点和自同态环.

定理 3.20 设 K 是特征 $p > 0$ 的完全域(perfect), E/K 是一椭圆曲线, 对每个 $r \geqslant 1$, 令

$$\phi_r: \quad E \longrightarrow E^{(p^r)}, \qquad \widehat{\phi}_r: \quad E^{(p^r)} \longrightarrow E$$

是 p^r 次幂 Frobenuis 映射及其对偶($E^{(p^r)}$ 是将 E 的 Weierstrass 方程的系数提升 p^r 次幂而得到的椭圆曲线), 则

(a) 下面的结论是等价的:

(i) $E[p^r] = 0$, 对一个(所有)$r \geqslant 1$;

(ii) $\widehat{\phi}_r$ 是(纯)不可分的, 对一个(所有)$r \geqslant 1$;

(iii) 映射 $[p] : E \to E$ 是纯不可分的且 $j(E) \in \mathbb{F}_{p^2}$;

(iv) $\mathrm{End}(E)$ 是四元数代数的一个阶;

(v) 形式群 $\widehat{E}/K$ 具有高度 2 (形式群的定义见第七章).

(b) 若(a)的等价条件不成立, 则

$$E[p^r] \simeq \mathbb{Z}/p^r\mathbb{Z}, \quad 对所有 r \geqslant 1,$$

且形式群 $\widehat{E}/K$ 有高度 1, 进一步, 若 $j(E) \in \overline{\mathbb{F}}_p$, 则 $\mathrm{End}(E)$ 是虚二次域的一个阶, 若 $j(E) \notin \overline{\mathbb{F}}_p$, 则 $\mathrm{End}(E) = \mathbb{Z}$.

证明见文献 [12].

定义 3.2 若 E 具有定理 3.20(a) 中的性质, 则称 E 是超奇异的, 且 E 具有 Hasse 不变量 0, 否则称 E 是正常 (ordinary) 的, 且 E 具有 Hasse 不变量 1.

由定理 3.20(a), 在同构意义下, 在 K 上仅存在有限条超奇异椭圆曲线 (或 Hasse 不变量 0), 因为每一条这样曲线的 j 不变量属于 $\mathbb{F}_{p^2}$. 对 $p=2$, 易知仅有超奇异椭圆曲线为

$$E: \quad y^2+y=x^3.$$

对 $p>2$, 下面定理给出了判定超奇异性的一个简单办法:

定理 3.21 设 $\mathrm{ch}(K)=p>2$,

(a) 设 E/K 具有Weierstrass方程

$$E: \quad y^2=f(x), \qquad f(x)\in K[x],$$

则 E 是超奇异的当且仅当 $f(x)^{(p-1)/2}$ 中 x^{p-1} 的系数为 0;

(b) 令 $m=(p-1)/2$, 定义多项式 $H_p(t)=\sum_{i=0}^{m}\binom{m}{i}^2 t^i$ 而 $\lambda\in\overline{K}$, $\lambda\neq 0,1$, 则椭圆曲线

$$E: \quad y^2=x(x-1)(x-\lambda)$$

超奇异 $\Longleftrightarrow$ $H_p(\lambda)=0$;

(c) $H_p(t)$ 在 $\overline{K}$ 中有不同的根, 在同构意义下, 恰好存在 $[p/12]+\varepsilon_p$ 条超奇异椭圆曲线, 其中 $\varepsilon_3=1$, 对 $p\geqslant 5$, 有

$$\varepsilon_p=0,\ 1,\ 1,\ 2 \quad 若 p\equiv 1,\ 5,\ 7,\ 11 \pmod{12}.$$

证明 (a) 设 $q=\#K$, 而 $\chi: K^\star\to\{\pm 1\}$ 是阶 2 的非平凡特征, 扩充 χ 到 K ($\chi(0)=0$), 即 $\chi(a)=1$ 当且仅当 a 是 $K^\star$ 中一个平方, 于是对每一个 $x\in K$, 若 $f(x)$ 是非平方 (分别是 0, 非 0 平方), 将产生 0 个 (分别是 1 个和 2 个) 点 $(x,y)\in E(K)$, 于是有

$$\#E(K)=1+\sum_{x\in K}\big(\chi(f(x))+1\big)=1+q+\sum_{x\in K}\chi\big(f(x)\big).$$

因 $K^\star$ 是 $q-1$ 阶循环群, 对任意 $z\in K$, 有

$$\chi(z)=z^{(q-1)/2} \quad (在\ K\ 中),$$

故

$$\#E(K)=1+\sum_{x\in K}f(x)^{(q-1)/2} \quad (在\ K\ 中),$$

但由于 K^* 的循环性, 易知

$$\sum_{x \in K} = \begin{cases} -1, & 若\ q-1 | i, \\ 0, & 若\ q-1 \nmid i. \end{cases}$$

因 $f(x)$ 次数为 3, 若乘出 $f(x)^{(q-1)/2}$ 并在 K 上求和, 仅有的非 0 项来自 x^{q-1}, 令 $A_q = f(x)^{(q-1)/2}$ 中x^{q-1} 的系数, 则

$$\#E(K) = 1 + A_q \qquad (在\ K\ 中).$$

另一方面, 设 $\phi: E \to E$ 是 q 次 Frobenius, 则

$$\#E(K) = \deg(1-\phi) = 1 - a + q,$$

其中 $a = \operatorname{tr}(\phi_l) = 1 - \deg(1-\phi) + \deg(\phi) = 1 - \widehat{(1-\phi)} \circ (1-\phi) + \widehat{\phi} \circ \phi = \phi + \widehat{\phi}$ (定理 3.19), 比较 $\#E(K)$ 的两个表达式, 知

$$-a = A_q \qquad (在\ K\ 中),$$

但 a 为整数, 故

$$A_q = 0 \iff a \equiv 0 \pmod p,$$

但 $\widehat{\phi} = [a] - \phi$, 故

$$\begin{aligned} a \equiv 0 \pmod p &\iff \widehat{\phi}是不可分的\ (命题\ 3.9) \\ &\iff E是超奇异的\ (定理\ 3.20(\mathrm{a(iii)})), \end{aligned}$$

即 $A_q = 0 \iff E$ 超奇异. 下证 $A_q = 0 \iff A_p = 0$, 写

$$\big(f(x)\big)^{(p^{r+1}-1)/2} = \big(f(x)^{(p^r-1)/2}\big)^{p^r},$$

注意 $f(x)$ 为 3 次, 比较两端系数, 有 $A_{p^{r+1}} = A_{p^r}(A_p)^{p^r}$ 于是利用归纳法知 $A_q = 0 \iff A_p = 0$.

(b) 这是 (a) 的特殊情形, 需要计算 $\big(x(x-1)(x-\lambda)\big)^m$ 的 x^{p-1} 的系数, 即 $\big(x(x-1)(x-\lambda)\big)^m$ 中 x^m 的系数, 这个系数为

$$\sum_{i=0}^{m} \binom{m}{i} (-\lambda)^i \binom{m}{m-1} (-1)^{m-i} = (-1)^m H_p(\lambda).$$

(c) 设 $\mathfrak{D}$ 是如下的微分算子:

$$\mathfrak{D}=4t(1-t)\frac{\mathrm{d}^2}{\mathrm{d}t^2}+4(1-2t)\frac{d}{dt}-1.$$

则直接计算表明

$$\mathfrak{D}H_p(t)=p\sum_{i=0}^{m}(p-2-2i)\binom{m}{i}^2t^i.$$

由于 $\mathrm{Char}(K)=p$, 故

$$\mathfrak{D}H_p(t)=0\quad(\text{在 } k[t] \text{ 中}).$$

因此 $H_p(t)$ 在 $\overline{K}$ 中仅有的重根只可能是 $t=0$ 和 $t=1$. 但是

$$H_p(0)=1,\quad H_p(1)=\binom{p-1}{m}\equiv(-1)^m\pmod p,$$

所以 $H_p(t)$ 的根是互不相同的, $H_p(t)$ 的每一个根 λ 将给出一条椭圆曲线

$$E_\lambda:\quad y^2=x(x-1)(x-\lambda).$$

对于 $p=3$, 有 $H_p(t)=1+t$. 因此存在恰有一条超奇异椭圆曲线, 其 j 不变量 $j(-1)=1728=0$. 假定 $p\geqslant 5$, 则易知映射 $\lambda\to j(\lambda)=2^8\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$ 在 $j\neq 0$, 1728 时是六对一的, 而 $j=0$ 时是二对一的, $j=1728$ 时是三对一的. 如果 $H_p(\lambda)=0$, 则对于满足 $j(\lambda')=j(\lambda)$ 的每一个 λ', 也一定有 $H_p(\lambda')=0$(因 $H_p(\lambda)=0$ 和已证明的 (b) 意味着 E_λ 是超奇异的, 而 $E_\lambda\cong E_{\lambda'}$, 于是 $E_{\lambda'}$ 也是超奇异的, 再由 (b) 知 $H_p(\lambda')=0$). 对于 $\mathbb{F}_p$ 上 j 不变量为 j 的椭圆曲线, 按照它们是否为超奇异的, 分别令 $\varepsilon_p(j)=1$ 或 0. 由于 $H_p(t)$ 具有不同的根, 因此, 当特征 $p\geqslant 5$ 时, 超奇异椭圆曲线的数量应当是

$$\begin{aligned}&\frac{1}{6}\left(\frac{p-1}{2}-2\varepsilon_p(0)-3\varepsilon_p(1728)\right)+\varepsilon_p(0)+\varepsilon_p(1728)\\=&\frac{p-1}{12}+\frac{2}{3}\varepsilon_p(0)+\frac{1}{2}\varepsilon_p(1728).\end{aligned}$$

直接计算不难看出

$$\varepsilon_p(0)=\begin{cases}0, & \text{若}\quad p\equiv 1\ (\mathrm{mod}\ 3),\\ 1, & \text{若}\quad p\equiv 2\ (\mathrm{mod}\ 3);\end{cases}$$

$$\varepsilon_p(1728)=\begin{cases}0, & \text{若}\quad p\equiv 1\ (\mathrm{mod}\ 4),\\ 1, & \text{若}\quad p\equiv 3\ (\mathrm{mod}\ 4);\end{cases}$$

由此即可证得定理.

第四章　复乘理论与算法

§4.1　椭圆曲线的复乘理论

在本节中, 我们简单地介绍椭圆曲线的复乘理论, 从而为下一节利用复乘理论来生成椭圆曲线的方法奠定理论基础.

现在, 给定 $\mathbb{C}$ 上椭圆曲线的一个 j 不变量, 则在同构意义下, 该椭圆曲线由下列方程给出:

$$\begin{aligned}&\text{若 } j=0,\ \text{则 } E:\ y^2=x^3-1,\\&\text{若 } j=1728,\ \text{则 } E:\ y^2=x^3-x,\\&\text{若 } j\neq 0,1728,\ \text{令 } c=j/(-j+1728),\ \text{则 } E:\ y^2=x^3+3cx+2c.\end{aligned}\tag{4.1}$$

考虑椭圆曲线 E 的自同态环 $\mathrm{End}(E)$, 如果 E 是非超奇异的, 则 $\mathrm{End}(E)$ 或者等于 $\mathbb{Z}$, 或者是一个虚二次域的阶 (order). 如果 $\mathrm{End}(E)\supsetneq\mathbb{Z}$, 则称 E 具有复乘. 因此, 当 E 具有复乘时, 有

$$\mathrm{End}(E)\cong\mathbb{Z}+\mathbb{Z}\tau,$$

其中 τ 是上半平面中一个二次复代数数.

复乘理论与 j 不变量之间的一个基本联系是下面的

定理 4.1　设 $\tau\in\mathfrak{H}$ 是一个二次代数数, 令 $E_\tau=\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$, 则

(1) $\mathrm{End}(E_\tau)$ 是 $\mathbb{Q}(\tau)$ 中的一个阶, 故 E_τ 具有复乘.

(2) $j(\tau)=j(E_\tau)$ 是一个代数整数.

证明　(1) 令 $L=\mathbb{Z}+\mathbb{Z}\tau$, 而 $\lambda\in\mathrm{End}(E_\tau)$, 则 λ 必定由一个满足条件 $\alpha L\subseteq L$ 的复数 α 诱导出来, 从而存在整数 a,b,c,d, 使得

$$\begin{cases}\alpha=a+b\tau,\\ \alpha\tau=c+d\tau,\end{cases}\tag{4.2}$$

于是由上面第一式知 $\alpha\in\mathbb{Q}(\tau)$. 下证必存在复数 $\alpha\notin\mathbb{Z}$, 使得 $\alpha L\subseteq L$. 事实上, 因为 τ 是二次代数数, 故存在 $a,b,c\in\mathbb{Z}$ $(a\neq 0)$, 使得

$$a\tau^2+b\tau+c=0.$$

现在显然有 $a\tau L \subseteq L$, 故 $\alpha = a\tau \in \mathrm{End}(E_\tau)$. 另一方面, 由 (4.2) 式消去 τ, 得

$$\alpha^2 - (a+d)\alpha + bc = 0.$$

可见 $\mathrm{End}(E_\tau) \subseteq \mathbb{Q}(\tau)$ 是 $\mathbb{Z}$ 的一个整扩张, 从而 $\mathrm{End}(E_\tau)$ 是 $\mathbb{Q}(\tau)$ 的一个阶, 于是 E_τ 有复乘.

(2) 这一部分的证明需要用到模多项式的性质. 设 $j(\tau)$ 是 j 不变量模函数, 则模多项式 $\Phi_n(X,j)$ 是 $\mathbb{C}(j)$ 上的不可约多项式. 而由 $\Phi_n(X,j)$ 的定义:

$$\Phi_n(X) := \Phi_n(X,j) = \prod_{i=1}^{\psi(n)} (X - j\circ\alpha_i),$$

其中 $\{\alpha_i | 0 \leqslant i \leqslant \psi(n)\}$ 是

$$\Delta_n^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2^+(\mathbb{Z}) \middle| \det\begin{pmatrix} a & b \\ c & d \end{pmatrix} = n,\ (a,b,c,d)=1 \right\}.$$

关于

$$\Gamma = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| ad - bc = 1 \right\}$$

的一个右陪集完全代表元集, $\psi(n) = n\prod_{p|n}\left(1+\frac{1}{p}\right)$.

于是可知对任意的 $\alpha \in M_2^+(\mathbb{Z})$, 函数 $j\circ\alpha$ 在 $\mathbb{Z}[j]$ 上整 (因 $j\circ\alpha$ 是 $\Phi_n(X)$ 的一个根, $n = \det(\alpha)$).

现在令 $K = \mathbb{Q}(\tau)$, 而 $\mathfrak{O}\mathbb{Z} + \mathbb{Z}z$ 是 K 中代数整数环. 我们总能找到 $\lambda \in \mathfrak{O}$, 使得 λ 的范数是无平方因子的: 若 $K = \mathbb{Q}[i]$, 可取 $\lambda = 1+i$, 若 $K = \mathbb{Q}(\sqrt{-m})$, $m > 1$ 无平方因子, 则可取 $\lambda = \sqrt{-m}$, 从而

$$\lambda z = az + b, \quad \lambda = cz + d, \qquad a,b,c,d \in \mathbb{Z},$$

而且 λ 的范数等于行列式 $ad - bc$. 令 $n = ad - bc$, 则

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Delta_n^*, \qquad \alpha z = z,$$

因此 $j(z)$ 是多项式 $\Phi_n(X,X)$ 的一个根. 但 $\Phi_n(X,X)$ 当 n 无平方因子时是一个首一的整系数多项式, 从而 $j(z)$ 是一个代数整数. 但 $\mathbb{Q}(z) = \mathbb{Q}(\tau)$, 故 $\tau = uz + v$, $u, v \in \mathbb{Q}$, 所以 $\tau = \beta z$, $\beta \in M_2^+(\mathbb{Z})$ 是本原的 (即 β 的各位置元素之最大公因子为 1). 由前面的讨论, $j\circ\beta$ 在 $\mathbb{Z}[j]$ 上整, 从而 $j(\beta z) = j(\tau)$ 在 $\mathbb{Z}[j(z)]$ 上整, 而 $j(z)$ 是代数整数, 故 $j(\tau)$ 亦然, 证毕.

我们下面的任务是：对于一个给定的复二次代数数 $\tau \in \mathfrak{H}$，找出 $j(\tau)$ 在 $\mathbb{Q}$ 上的极小多项式，这个极小多项式的存在性由上面的定理 4.1 保证. 首先给出几个记号：设 K 是一个虚二次域，R_K 是其整数环，$CL(R_K)$ 是 R_K 的理想类群，即

$$CL(R_K) = \{K\text{的非零分式理想}\}/\{K\text{的非零主理想}\}.$$

最后，令 $EC(R_K)$ 是自同态环为 R_K 的椭圆曲线的同构类的集合，即

$$\begin{aligned} EC(R_K) &= \{\text{椭圆曲线 } E/\mathbb{C} \mid \mathrm{End}(E) \cong R_K\}/\mathbb{C}\text{上的同构} \\ &= \{\mathbb{C}\text{上的格 } \wedge \mid \mathrm{End}(E_\wedge) \cong R_K\}/\mathbb{C}\text{上的相似}. \end{aligned}$$

下面来看 $CL(R_K)$ 和 $EC(R_K)$ 之间的密切联系：设 $\mathfrak{a}$ 是 R_K 中的一个非零分式理想，应用嵌入，$\mathfrak{a} \subset K \subset \mathbb{C}$，可以将 $\mathfrak{a}$ 视为 $\mathbb{C}$ 中一个格，从而有一条对应于 $\mathfrak{a}$ 的椭圆曲线 $E_\mathfrak{a}$，其自同态环为

$$\begin{aligned} \mathrm{End}(E_\mathfrak{a}) &\cong \{\alpha \in \mathbb{C} \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} = \{\alpha \in K \mid \alpha\mathfrak{a} \subset \mathfrak{a}\} \quad (\text{因 } \mathfrak{a} \subset K) \\ &= R_K \quad (\text{因 } \mathfrak{a}\text{是分式理想}). \end{aligned}$$

于是 K 中任何非零分式理想都给出一条具有复乘 R_K 的椭圆曲线. 另一方面，相似的格给出同构的椭圆曲线，故 $\mathfrak{a}$ 和 $c\mathfrak{a}$ 给出 $EC(R_K)$ 中相同的椭圆曲线. 于是有一个映射 ($\bar{\mathfrak{a}}$ 表示 $\mathfrak{a}$ 所在的理想类)

$$CL(R_K) \to EC(R_K), \qquad \bar{\mathfrak{a}} \mapsto E_\mathfrak{a}.$$

另一方面，定义 $CL(R_K)$ 在 $EC(R_K)$ 上的一个作用如下：对任意格 $\wedge$ (使得 $E_\wedge \in EC(R_K)$) 和任意的分式理想 $\mathfrak{a}$，记

$$\mathfrak{a}\wedge = \left\{\sum \alpha_i\lambda_i \mid \alpha_i \in \mathfrak{a},\ \lambda_i \in \wedge\right\}.$$

下面将证明 $\mathfrak{a}\wedge$ 是 $\mathbb{C}$ 中的一个格，$\mathrm{End}(E_{\mathfrak{a}\wedge}) \cong R_K$，且 $E_{\mathfrak{a}\wedge} \cong E_{\mathfrak{P}\wedge}$ 当且仅当 $\bar{\mathfrak{a}} = \overline{\mathfrak{P}}$，从而可以得到 $CL(R_K)$ 在 $EC(R_K)$ 上的一个作用. 下述定理给出了这个作用的一些性质：

定理 4.2 (a) 设 $\wedge$ 是 $\mathbb{C}$ 中一个格，使得 $E_\wedge \in EC(R_K)$，令 $\mathfrak{a}$ 和 $\mathfrak{P}$ 是 K 的非零分式理想，则

(i) $\mathfrak{a}\wedge$ 是 $\mathbb{C}$ 中一个格；

(ii) $\mathrm{End}(E_{\mathfrak{a}\wedge}) \cong R_K$；

(iii) $E_{\mathfrak{a}\wedge} \cong E_{\mathfrak{P}\wedge}$ 当且仅当 $\bar{\mathfrak{a}} = \overline{\mathfrak{P}}$；

从而 $CL(R_K)$ 在 $EC(R_K)$ 上定义了一个作用如下：

$$\bar{\mathfrak{a}} \star E_\wedge = E_{\mathfrak{a}^{-1}\wedge}.$$

(b) 上述 $CL(R_K)$ 在 $EC(R_K)$ 中的作用是简单传递的. 特别地, 有

$$\#CL(R_K) = \#EC(R_K).$$

证明 (a) (i) 由假设, $\mathrm{End}(E_\Lambda) = R_K$, 故 $R_K\Lambda = \Lambda$. 选取非零整数 $d \in \mathbb{Z}$, 使得 $d\mathfrak{a} \subset R_K$, 则 $\mathfrak{a}\Lambda \subset \frac{1}{d}\Lambda$, 从而 $\mathfrak{a}\Lambda$ 是 $\mathbb{C}$ 之离散子群. 类似地, 选取非零整数 d, 使得 $dR_K \subset \mathfrak{a}$, 则 $d\Lambda \subset \mathfrak{a}\Lambda$, 从而 $\mathfrak{a}\Lambda$ 张成 $\mathbb{C}$, 故 $\mathfrak{a}\Lambda$ 是一个格.

(ii) 对任意 $\alpha \in \mathbb{C}$ 和任意非零分式理想 $\mathfrak{a}$, 有

$$\alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda \iff \mathfrak{a}^{-1}\alpha\mathfrak{a} \subset \mathfrak{a}^{-1}\mathfrak{a}\Lambda \iff \alpha\Lambda \subset \Lambda,$$

$$\mathrm{End}(E_{\mathfrak{a}\Lambda}) = \{\alpha \in \mathbb{C} \,|\, \alpha\mathfrak{a}\Lambda \subset \mathfrak{a}\Lambda\} = \{\alpha \in \mathbb{C} \,|\, \alpha\Lambda \subset \Lambda\} = \mathrm{End}(E_\Lambda) = R_K.$$

(iii) 由于 $E_{\mathfrak{a}\Lambda}$ 的同构类由 $\mathfrak{a}\Lambda$ 的相似类决定, 即 $E_{\mathfrak{a}\Lambda} = E_{\mathfrak{P}\Lambda}$ 当且仅当存在 $c \in \mathbb{C}^*$, 使得 $\mathfrak{a}\Lambda = c\mathfrak{P}\Lambda$. 两边乘上 $\mathfrak{a}^{-1}$, 注意到 $R_K\Lambda = \Lambda$, 则

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{P}\Lambda} \iff \Lambda = c\mathfrak{a}^{-1}\mathfrak{P}\,\Lambda\,.$$

类似地, 乘上 $c^{-1}\mathfrak{P}^{-1}$, 可知

$$E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{P}\Lambda} \iff \Lambda = c^{-1}\mathfrak{a}\mathfrak{P}^{-1}\,\Lambda\,.$$

因此, 若 $E_{\mathfrak{a}\Lambda} \cong E_{\mathfrak{P}\Lambda}$, 则 $c\mathfrak{a}^{-1}\mathfrak{P}$ 和 $c^{-1}\mathfrak{a}\mathfrak{P}^{-1}$ 都将 Λ 变到 Λ, 从而它们都包含在 R_K 中, 都等于 R_K, 于是 $\mathfrak{a} = c\mathfrak{P}$, 从而 $c \in K$, 且 $\bar{\mathfrak{a}} = \bar{\mathfrak{P}}$. 这就证明了 (iii).

最后, 由

$$\bar{\mathfrak{a}} * (\bar{\mathfrak{P}} * E_\Lambda) = \bar{\mathfrak{a}} * E_{\mathfrak{P}^{-1}\Lambda} = E_{\mathfrak{a}^{-1}(\mathfrak{P}^{-1}\Lambda)} = E_{(\mathfrak{a}\mathfrak{P})^{-1}\Lambda} = (\overline{\mathfrak{a}\mathfrak{P}}) * E_\Lambda$$

知 $\bar{\mathfrak{a}} * E_\Lambda = E_{\mathfrak{a}^{-1}\Lambda}$ 给出了一个群作用.

(b) 设 E_{Λ_1} 和 $E_{\Lambda_2} \in EC(R_K)$, 我们必须找出 $\bar{\mathfrak{a}} \in CL(R_K)$, 使得 $\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\Lambda_2}$. 任取 $0 \neq \lambda_1 \in \Lambda_1$, 令 $\mathfrak{a}_1 = \frac{1}{\lambda_1}\Lambda_1$, 则 $\mathfrak{a}_1 \subset K$ 且是有限生成的 R_K 模, 故 $\mathfrak{a}_1$ 是 K 的一个分式理想. 类似地, 任取 $\lambda_2 \in \Lambda_2$, 有分式理想 $\mathfrak{a}_2 = \frac{1}{\lambda_2}\Lambda_2$, 则

$$\frac{\lambda_2}{\lambda_1}\mathfrak{a}_2\mathfrak{a}_1^{-1}\Lambda_2 = \Lambda_2.$$

因此, 若令 $\mathfrak{a} = \mathfrak{a}_2^{-1}\mathfrak{a}_1$, 则

$$\bar{\mathfrak{a}} * E_{\Lambda_1} = E_{\mathfrak{a}^{-1}\Lambda_1} = E_{\frac{\lambda_1}{\lambda_2}\Lambda_2} \cong E_{\Lambda_2}.$$

这就证明了作用是传递的. 为了证明作用的单性, 就必须说明: 若 $\mathfrak{a} * E_\wedge = \mathfrak{P} * E_\wedge$, 则 $\bar{\mathfrak{a}} = \overline{\mathfrak{P}}$, 这正是 (a) 中的 (ii), 证毕.

下面研究复乘椭圆曲线的定义域和自同态. 事实上, 由定理 4.1 可知, 具有复乘的椭圆曲线一定定义在 $\mathbb{Q}$ 的一个代数扩张上. 事实上, 有

定理 4.3 (a) 设 $E/\mathbb{C}$ 是椭圆曲线, $\sigma: \mathbb{C} \to \mathbb{C}$ 是 $\mathbb{C}$ 的任意的域自同构, 则

$$\mathrm{End}(E^\sigma) \cong \mathrm{End}(E).$$

(b) 设 $E/\mathbb{C} \in EC(R_K)$, 则 $j(E)$ 是代数整数, 且 $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leqslant h(K)$, $h(K)$ 是 K 的类数.

(c) $EC(R_K) \cong \{$椭圆曲线 $E/\overline{\mathbb{Q}} \,|\, \mathrm{End}(E) \cong R_K\}/\overline{\mathbb{Q}}$ 上的同构.

证明 (a) 显然.

(b) 由定理 4.1, 知 $j(E)$ 是代数整数. 现在设 $\sigma \in \mathrm{Aut}(\mathbb{C})$. E^σ 是 σ 作用在 E 上 Weierstrass 方程系数上而获得的椭圆曲线, 由于 j 不变量是系数的有理函数, 故 $j(E^\sigma) = j(E)^\sigma$. 而 (a) 表明 $\mathrm{End}(E^\sigma) \cong R_K$, 故由定理 4.2(b) 知, $E^\sigma \in EC(R_K)$, 但 $\#EC(R_K) = \#CL(R_K)$, 故当 σ 跑遍 $\mathrm{Aut}(\mathbb{C})$ 时, E^σ 只能在 $EC(R_K)$ 的有限个 (个数 $\leqslant \#CL(R_K)$) $\mathbb{C}$ 同构类中. 从而当 σ 跑遍 $\mathrm{Aut}(\mathbb{C})$ 时, $j(E)^\sigma = j(E^\sigma)$ 只能取到有限个值, 且取值的可能性不大于 $\#CL(R_K)$, 从而 $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leqslant h(K)$.

(c) 对 $\mathbb{C}$ 的任意子域 $\mathbb{F}$, 令

$$EC_{\mathbb{F}}(R_K) = \{\text{椭圆曲线 } E/\mathbb{F} \,|\, \mathrm{End}(E) \cong R_K\}/\mathbb{F}\text{上的同构}.$$

固定一个嵌入 $\overline{\mathbb{Q}} \hookrightarrow \mathbb{C}$, 则存在自然的映射

$$\varphi: \ EC_{\overline{\mathbb{Q}}} \to EC(R_K).$$

要证 φ 是一个一一对应.

令 $E/\mathbb{C} \in EC(R_K)$, 则有

(1) $j(E) \in \overline{\mathbb{Q}}$;

(2) 存在椭圆曲线 $E'/\mathbb{Q}(j(E))$, 使得 $j(E') = j(E)$(由 4.1 式);

(3) E' 与 E 在 $\mathbb{C}$ 上同构.

可见 $\varphi(E') = E$, 故 φ 是满的. 又设 $E_1/\overline{\mathbb{Q}}$, $E_2/\overline{\mathbb{Q}} \in EC_{\overline{\mathbb{Q}}}(R_K)$, 且 $\varphi(E_1) = \varphi(E_2)$, 则 $j(E_1) = j(E_2) \in \overline{\mathbb{Q}}$, 于是由 (4.1) 式知 E_1 和 E_2 在 $\overline{\mathbb{Q}}$ 上同构, 因此 $E_1/\overline{\mathbb{Q}} = E_2/\overline{\mathbb{Q}} \in EC_{\overline{\mathbb{Q}}}(R_K)$, 故 φ 是单的, 证毕.

由定理 4.3(c), 可以将 $EC(R_K)$ 等同于具有复乘 R_K 的椭圆曲线的 $\overline{\mathbb{Q}}$ 同构类. 于是, 存在 $\mathrm{Gal}(\overline{K}/K)$ 在 $EC(R_K)$ 上的一个自然作用: 任意 $\sigma \in \mathrm{Gal}(\overline{K}/K)$ 将 E 的

同构类映到 E^σ 的同构类. 另一方面, 由定理 4.2(b), 类群 $CL(R_K)$ 在 $EC(R_K)$ 上的作用是单传递的, 故存在惟一的 $\overline{\mathfrak{A}} \in CL(R_K)$, 使得

$$\overline{\mathfrak{A}} \star E = E^\sigma.$$

换言之, 存在映射

$$\psi:\ \mathrm{Gal}(\overline{K}/K) \to CL(R_K),$$

使得对任意的 $\sigma \in \mathrm{Gal}(\overline{K}/K)$, 有

$$E^\sigma = \psi(\sigma) \star E,$$

通过对 ψ 的精细研究, 能够精确地描述域 $K\big(j(E)\big)$. 首先, 证明 ψ 是一个同态.

定理 4.4 设 $K/\mathbb{Q}$ 是一个虚二次域, 则存在一个同态

$$\psi:\ \mathrm{Gal}(\overline{K}/K) \to CL(R_K),$$

由下列条件所惟一刻画:

$$E^\sigma = \psi(\sigma) \star E, \quad \forall \sigma \in \mathrm{Gal}(\overline{K}/K), \forall E \in EC(R_K).$$

证明 由上面的描述知, 对任一条固定的 $E \in EC(R_K)$, 我们有一个良好定义的映射

$$\psi:\ \mathrm{Gal}(\overline{K}/K) \to CL(R_K),$$

它由性质 $E^\sigma = \psi(\sigma) \star E$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$ 所决定. 因为

$$\begin{aligned}\psi(\sigma\tau) \star E = E^{\sigma\tau} &= \big(E^\sigma\big)^\tau = \big(\psi(\tau) \star E\big)^\sigma \\ &= \psi(\sigma) \star \big(\psi(\tau) \star E\big) = \big(\psi(\sigma)\psi(\tau)\big) \star E,\end{aligned}$$

故 ψ 是一个同态.

剩下要证明的是 ψ 的定义与 $EC(R_K)$ 中元素的选取无关. 设 $E_1, E_2 \in EC(R_K)$, $\sigma \in \mathrm{Gal}(\overline{K}/K)$, 令 $E_1^\sigma = \overline{\mathfrak{A}}_1 \star E_1$, $E_2^\sigma = \overline{\mathfrak{A}}_2 \star E_2$, 我们要证明 $\overline{\mathfrak{A}}_1 = \overline{\mathfrak{A}}_2$. 因 $CL(R_K)$ 传递作用于 $EC(R_K)$, 存在某个 $\bar{b}$, 使得 $E_2 = \bar{b} \star E_1$, 故

$$\big(\bar{b} \star E_1\big)^\sigma = E_2^\sigma = \overline{\mathfrak{A}}_2 \star E_2 = \overline{\mathfrak{A}}_2 \star (\bar{b} \star E_1) = \big(\overline{\mathfrak{A}}_2 \bar{b}\, \overline{\mathfrak{A}}_1^{-1}\big) \star E_1^\sigma.$$

因此, 若能证明 $(\bar{b} \star E_1)^\sigma = \bar{b} \star E_1^\sigma$, 则有 $E_1^\sigma = \big(\overline{\mathfrak{A}}_2 \overline{\mathfrak{A}}_1^{-1}\big) \star E_1^\sigma$, 再由定理 4.2(b), 知 $\overline{\mathfrak{A}}_2 = \overline{\mathfrak{A}}_1$. 于是完成了定理的证明, 所以只要证明下面的引理 4.1 即可完成定理 4.4 的证明.

引理 4.1　设 $E/\overline{Q}$ 是代表 $EC(R_K)$ 中一个元素的椭圆曲线. $\overline{\mathfrak{A}} \in CL(R_K)$, $\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, 则

$$\left(\overline{\mathfrak{A}} \star E\right)^{\sigma} = \overline{\mathfrak{A}}^{\sigma} \star E^{\sigma}.$$

证明　选取一个格 $\wedge$, 使得 $E \cong E_{\wedge}$, 并固定一个正合列

$$R_K^m \xrightarrow{\ A\ } R_K^n \longrightarrow \mathfrak{A} \longrightarrow 0, \tag{4.3}$$

其中 $A \in M_{m\times n}(R_K)$. 我们还有下述正合列:

$$0 \longrightarrow \wedge \longrightarrow \mathbb{C} \longrightarrow E \longrightarrow 0. \tag{4.4}$$

将 Hom 函子用到 (4.3) 和 (4.4) 式, 有下列交换图表:

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(\mathfrak{A},\wedge) & \longrightarrow & \mathrm{Hom}(\mathfrak{A},\mathbb{C}) & \longrightarrow & \mathrm{Hom}(\mathfrak{A}_1,E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(R_K^n,\wedge) & \longrightarrow & \mathrm{Hom}(R_K^n,\mathbb{C}) & \longrightarrow & \mathrm{Hom}(R_K^n,E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathrm{Hom}(R_K^m,\wedge) & \longrightarrow & \mathrm{Hom}(R_K^m,\mathbb{C}) & \longrightarrow & \mathrm{Hom}(R_K^m,E)
\end{array} \tag{4.5}$$

此处 Hom 表示 R_K 模的同态. 对任意 R_K 模 M, 有 $\mathrm{Hom}(R_K^n, M) \cong M^n$. 另一方面, 对任意的分式理想 $\mathfrak{A}$ 和无扭 R_K 模 M, 不难验证自然映射

$$\begin{aligned}
\phi:\quad \mathfrak{A}^{-1}M &\longrightarrow \mathrm{Hom}(\mathfrak{A}, M) \\
x\quad &\longmapsto (\phi_x:\ \alpha \mapsto \alpha x)
\end{aligned}$$

是一个同构, 于是 $\mathrm{Hom}(\mathfrak{A},\wedge) = \mathfrak{A}^{-1}\wedge$, $\mathrm{Hom}(\mathfrak{A},\mathbb{C}) = \mathfrak{A}^{-1}\mathbb{C} = C$. 于是 (4.5) 式变成

$$\begin{array}{ccccccc}
 & & 0 & & 0 & & 0 \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \mathfrak{A}^{-1}\wedge & \longrightarrow & \mathbb{C} & \longrightarrow & \mathrm{Hom}(\mathfrak{A}_1,E) \\
 & & \downarrow & & \downarrow & & \downarrow \\
0 & \longrightarrow & \wedge^n & \longrightarrow & \mathbb{C}^n & \longrightarrow & E^n \\
 & & \downarrow{\scriptstyle t_A} & & \downarrow{\scriptstyle t_A} & & \downarrow{\scriptstyle t_A} \\
0 & \longrightarrow & \wedge^m & \longrightarrow & \mathbb{C}^m & \longrightarrow & E^m
\end{array} \tag{4.6}$$

此处 t_A 是 A 的转置, 且由 (4.4) 式知后两行显然是正合的, 应用蛇形引理到 (4.6) 式的后两行, 得出正合列

$$0 \longrightarrow \mathfrak{A}^{-1}\wedge \longrightarrow \mathbb{C} \longrightarrow (\mathrm{Ker}:\ E^n \xrightarrow{t_A} E^m) \longrightarrow \wedge^n/t_A\wedge^m, \tag{4.7}$$

注意 $E^n \xrightarrow{t_A} E^m$ 是代数簇的一个代数映射, 故点 $(0,\cdots,0)\in E^m$ 的逆像是 E^n 的一个代数子簇. 又因为 E^n 和 E^m 是群簇, 故 $E^n \xrightarrow{t_A} E^m$ 的核是一个代数簇. 另一方面, 着眼于复拓扑知 $\wedge^n/t_A\wedge^m$ 是离散的, 而 $\mathbb{C}/\mathfrak{A}^{-1}\wedge$ 是连通的, 因此, 正合列 (4.7) 式给出

$$(\mathfrak{A}\star E)(\mathbb{C}) = \mathbb{C}/\mathfrak{A}^{-1}\wedge \cong \mathrm{Ker}(E^n \xrightarrow{t_A} E^m)\text{ 的单位分支},$$

因此, 我们给出了 $\mathfrak{A}\star E$ 的代数描述. 现在, 对任意的 $\sigma\in\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, 将 σ 应用到 E 和 E^σ 的上述刻画, 有

$$\begin{aligned}(\mathfrak{A}\star E)^\sigma &= \big(\mathrm{Ker}E^n \xrightarrow{t_A} E^m)\text{的单位分支}\big)^\sigma\\ &= \mathrm{Ker}\big((E^\sigma)^n \xrightarrow{t_A} (E^\sigma)^m\big)\text{的单位分支}\\ &= \mathfrak{A}^\sigma\star E^\sigma.\end{aligned}$$

这就完成了引理 4.1 的证明. 注意, 上面的第二个等号是由下面的引理 4.2(b) 得证的.

引理 4.2 (a) 设 $E/\mathbb{C}$ 是具有复乘 R 的椭圆曲线, 则存在惟一的同构

$$[\cdot]:\ R\cong\mathrm{End}(E),$$

使得对 E 的任意不变微分 $\omega\in\Omega_E$, 有

$$[\alpha]^*\omega=\alpha\omega,\quad \forall\alpha\in R.$$

(b) 对任意的 $\alpha\in R$, $\sigma\in\mathrm{Aut}(\mathbb{C})$, 有

$$[\alpha]_E^\sigma=\left[\alpha^\sigma\right]_{E^\sigma}.$$

证明 (a) 选取格 $\wedge$ 和同构 $E\cong E_\wedge$, 故只要对 $E_\wedge$ 证明 (a) 即可 (因为同构仅仅影响不变微分的一个非零常数倍). 于是 $E_\wedge$ 的自同态环同构到 $\{\alpha\in\mathbb{C}\,|\,\alpha\wedge\subset\wedge\}=R\subset\mathbb{C}$. 更精确地说, 每个 $\alpha\in R$ 给出一个自同态 $[\alpha]:\ E_\wedge\to E_\wedge$, 它由下述交换图表决定:

$$\begin{array}{ccc}\mathbb{C}/\wedge & \xrightarrow[z\mapsto\alpha z]{\phi_\alpha} & \mathbb{C}/\wedge\\ \downarrow f & & \downarrow f\\ E_\wedge & \xrightarrow{[\alpha]} & E_\wedge\end{array}$$

我们将证明这个映射 $[\cdot]: R \to \mathrm{End}(E_\wedge)$ 满足 $[\alpha]^*\omega = \alpha\omega$.

首先, 注意到 $E_\wedge$ 上任意两个非零不变微分只差一个常数倍, 因此, 若任取一个不变微分 $\omega \in \Omega_{E_\wedge}$, 并借助同构 $f: \mathbb{C}/\wedge \to E_\wedge(\mathbb{C})$, 我们将获得 $\mathbb{C}/\wedge$ 上不变微分 dz 的一个倍数: $f^*\omega = cdz$. 现在追踪上面的交换图表, 有

$$[\alpha]^*\omega = \left(f^{-1}\right)^* \circ \phi_\alpha^* \circ f^*(\omega) = \left(f^{-1}\right)^* \circ \phi_\alpha^*(cdz) = \left(f^{-1}\right)^*(c\alpha dz) = \alpha\omega.$$

(b) 设 $\omega \in \Omega_E$ 是非零不变微分, 则由 (a) 知

$$[\alpha]_E^*\omega = \alpha\omega, \qquad \forall \alpha \in R.$$

更进一步, 由于 ω^σ 是 E^σ 上一个不变微分, 再由 (a) 知

$$[\beta]_{E^\sigma}^*\omega^\sigma = \beta\omega^\sigma, \quad \forall \beta \in R.$$

现在对任意 $\alpha \in R$, $\sigma \in \mathrm{Aut}(\mathbb{C})$, 有

$$\left([\alpha]_E^\sigma\right)^*\left(\omega^\sigma\right) = \left([\alpha]_E^*\omega\right)^\sigma = (\alpha\omega)^\sigma = \alpha^\sigma\omega^\sigma = [\alpha^\sigma]_{E^\sigma}^*(\omega^\sigma),$$

这表明 $[\alpha]_E^\sigma$ 和 $[\alpha^\sigma]_{E^\sigma}$ 在不变微分 ω^σ 上有相同的作用. 由命题 3.6 知, 自然映射

$$\mathrm{End}(E^\sigma) \to \mathrm{End}(\Omega_{E^\sigma}), \quad \psi \mapsto \psi^*$$

是单的 (因此特征为 0, 所有有限映射均可分), 从而 $[\alpha]_E^\sigma = [\alpha^\sigma]_{E^\sigma}$, 证毕.

下面考虑同种映射在约化映射下的性状.

引理 4.3　*设 L 是一个数域, $\mathfrak{P}$ 是 L 的一个极大理想, E_1/L 和 E_2/L 是在 $\mathfrak{P}$ 处有好的约化的椭圆曲线, 而 $\widetilde{E}_1$ 和 $\widetilde{E}_2$ 是它们模 $\mathfrak{P}$ 的约化, 则自然的约化映射*

$$\mathrm{Hom}(E_1, E_2) \to \mathrm{Hom}(\widetilde{E}_1, \widetilde{E}_2), \quad \phi \mapsto \widetilde{\phi}$$

是单射且它保持次数, 即有 $\deg\phi = \deg\widetilde{\phi}$.

证明　因为一个非零同种的次数是非零的, 故引理 4.3 中映射的单性可由保次性得出. 下证 $\deg\phi = \deg\widetilde{\phi}$. 选取一个有理素理想 l, 使得 l 与 $\mathfrak{P}$ 互素, 利用 Weil 对的性质, 有: 对任意 $x, y \in T_l(E_1)$,

$$e_{E_1}(x,y)^{\deg\phi} = e_{E_1}\left((\deg\phi)x, y\right) = e_{E_1}\left(\widehat{\phi}\phi x, y\right) = e_{E_2}(\phi x, \phi y), \tag{4.8}$$

$$e_{\widetilde{E}_1}(\widetilde{x},\widetilde{y})^{\deg\widetilde{\phi}} = e_{\widetilde{E}_1}\left((\deg\widetilde{\phi})\widetilde{x}, \widetilde{y}\right) = e_{\widetilde{E}_1}\left(\widehat{\widetilde{\phi}}\widetilde{\phi}\widetilde{x}, \widetilde{y}\right) = e_{\widetilde{E}_2}(\widetilde{\phi}\widetilde{x}, \widetilde{\phi}\widetilde{y}). \tag{4.9}$$

若 E/L 是任意在 $\mathfrak{P}$ 具有好的约化的椭圆曲线, 则 $E[l^n] \cong \widetilde{E}[l^n]$(对一切 n), 从而有 $T_l(E) \cong T_l(\widetilde{E})$. 由 Weil 对的定义有

$$\widetilde{e_E(x,y)} = e_{\widetilde{E}}(\widetilde{x},\widetilde{y}), \quad \forall x, y \in T_l(E). \tag{4.10}$$

任取 $x,y\in T_l(E_1)$, 分别利用 (4.8) ~ (4.10) 式, 有

$$\begin{aligned}e_{\widetilde{E}_1}(\widetilde{x},\widetilde{y})^{\deg\phi}&=\widetilde{e_{E_1}(x,y)}^{\deg\phi}=\widetilde{e_{E_2}(\phi x,\phi y)}\\&=e_{\widetilde{E}_2}(\widetilde{\phi x},\widetilde{\phi y})=e_{\widetilde{E}_2}(\widetilde{\phi}\widetilde{x},\widetilde{\phi}\widetilde{y})=e_{\widetilde{E}_1}(\widetilde{x},\widetilde{y})^{\deg\widetilde{\phi}}.\end{aligned}$$

由于 $x,y\in T_l(E_1)$ 是任意的, 且 $T_l(\widetilde{E}_1)\cong T_l(E_1)$, 故上式对任意 $\widetilde{x},\widetilde{y}\in T_l(\widetilde{E}_1)$ 成立, 由 Weil 对的非退化性知 $\deg\phi=\deg\widetilde{\phi}$, 证毕.

现在回顾定理 4.4 中的同态 ψ:

$$\begin{aligned}\psi:\quad&\mathrm{Gal}(\overline{K}/K)\longrightarrow CL(R_K)\\&E^\sigma=\psi(\sigma)\star E,\quad\forall\sigma\in\mathrm{Aut}(\overline{K}/K),\ E\in EC(R_K).\end{aligned}$$

注意 ψ 的核实际上是 $\mathrm{Gal}(\overline{K}/K)$ 的一个有限商 (因为任意 E 可以定义在某个有限扩张 L/K 上, 于是 $\psi(\sigma)=1$ 对任意 $\sigma\in\mathrm{Gal}(\overline{K}/L)$ 成立), 又因为 $CL(R_K)$ 是 abelian 的, 故 ψ 可通过 $\psi:\ \mathrm{Gal}(K^{ab}/K)\to CL(R_K)$ 分解, 其中 K^{ab} 是 K 的最大 abelian 扩张. 令 $\mathfrak{p}$ 是 K 的一个素理想, 而 $\sigma_\mathfrak{p}\in\mathrm{Gal}(K^{ab}/K)$ 是对应 $\mathfrak{p}$ 的 Frobenius. 下面的命题是十分重要的:

命题 4.1 *存在有理素数的一个有限集合 $S\subset\mathbb{Z}$, 使得若 $p\notin S$ 是一个素数且在 K 中分裂, 即 $pR_K=\mathfrak{p}\mathfrak{p}'$, 则*

$$\psi(\sigma_\mathfrak{p})=\overline{\mathfrak{p}}\in CL(R_K).$$

证明 由于 $EC(R_K)$ 是有限的且其中每一条曲线均可定义在 $\overline{\mathbb{Q}}$ 上, 故可以选取一个有限扩张 L/K 和 $EC(R_K)$ 中 $\overline{K}$ 同构类的代表元 $E_1,E_2,\cdots,E_n$, 它们都定义在 L 上. 首先证明下述事实: 设 E_1/L 和 E_2/L 是定义在 L 上的椭圆曲线, 则存在一个有限扩张 L'/L, 使得从 E_1 到 E_2 的每一个同种都定义在 L' 上.

事实上, 因为 E_1/L 和 E_2/L 定义在 L 上, 故可取 E_1 和 E_2 的 Weierstras 方程, 其系数位于 L 中. 设 $\phi\in\mathrm{Hom}(E_1,E_2)$, 则对任意固定 L 的 $\sigma\in\mathrm{Aut}(\mathbb{C})$, 有 $\phi^\sigma\in\mathrm{Hom}(E_1,E_2)$, 注意 $\deg\phi^\sigma=\deg\phi$. 因为一个同种 $\phi\in\mathrm{Hom}(E_1,E_2)$ 由其核所决定到 E_1 及 E_2 的一个自同构, 而 E_1 只有有限个给定阶的有限阶子群, 且 $\mathrm{Aut}(E_1)$ 和 $\mathrm{Aut}(E_2)$ 有限, 故 $\mathrm{Hom}(E_1,E_2)$ 仅含有有限个给定次数的同种, 因此集合 $\{\phi^\sigma\,|\,\sigma\in\mathrm{Aut}(\mathbb{C}),\sigma固定L\}$ 是有限的, 这表明 ϕ 定义在 L 的一个有限扩张上. 又因为 $\mathrm{Hom}(E_1,E_2)$ 是有限生成的群, 故只要取 L' 是 $\mathrm{Hom}(E_1,E_2)$ 的生成元的有限集合的定义域即可.

由此, 通过由 L 的某个有限扩张替代 L, 可以假定 E_1, E_2, $\cdots$, E_n 相互之间的任意一个同种都定义在 L 上. 现在令 S 是满足下述条件的有理素数 p 的集合:

(1) p 在 L 中分歧;

(2) 某个 E_i 在位于 p 上的 L 的某个素理想处的约化是坏的;

(3) p 除尽某个 $N_{L/\mathbb{Q}}\big(j(E_i)-j(E_k)\big)$ $(i\neq k)$ 的分子或分母.

注意条件 (3) 意味着：若 $p\notin\mathcal{S}$ 且 $\mathfrak{P}\subset L$ 是整除 p 的一个素理想, 则 $\widetilde{E_i}\not\cong\widetilde{E_k}$ $(\bmod\ \mathfrak{P})$(因它们的 j 不变量模 $\mathfrak{P}$ 不同).

现设 $p\notin\mathcal{S}$, $pR_K=\mathfrak{p}\mathfrak{p}'$. 令 $\mathfrak{P}|\mathfrak{p}$, $\mathfrak{P}\subseteq L$ 是 L 中素理想, 令 $\wedge$ 是对应于 E 的一个格, 于是 $E(\mathbb{C})\cong\mathbb{C}/\wedge$. 选取整理想 $\mathfrak{a}\subset R_K$, 使得 $\mathfrak{a}$ 与 p 互素且 $\mathfrak{a}\mathfrak{p}=(\alpha)$ 是主理想, 于是存在连接 E, $\overline{\mathfrak{p}}\star E$ 和 $\overline{\mathfrak{a}}\star\overline{\mathfrak{p}}\star E$ 的同种, 使得有下面的交换图表：

$$\begin{array}{ccccccc}
\mathbb{C}/\wedge & \xrightarrow[z\to z]{} & \mathbb{C}/\mathfrak{p}^{-1}\wedge & \xrightarrow[z\to z]{} & \mathbb{C}/\mathfrak{a}^{-1}\mathfrak{p}^{-1}\wedge=\mathbb{C}/(\alpha^{-1})\wedge & \xrightarrow[z\to\alpha z]{} & \mathbb{C}/\wedge\\
\downarrow & & \downarrow & & \downarrow & & \downarrow\\
E & \xrightarrow{\phi} & \overline{\mathfrak{p}}\star E & \xrightarrow{\psi} & \overline{\mathfrak{a}}\star\overline{\mathfrak{p}}\star E=(\alpha)\star E & \xrightarrow[\sim]{\lambda} & E
\end{array}\tag{4.11}$$

现在选取 E/L 的一个 Weierstrass 方程, 使其在 $\mathfrak{P}$ 是极小的, 令 $\omega=\frac{dx}{2y+a_1x+a_2}$ 是 E 上的不变微分. ω 在 $\mathbb{C}/\wedge$ 上的约化是 dz 的一个倍数. 因上述图表 (4.11) 的上面一行映射的复合是 $z\to\alpha z$, 故 dz 将约化到 $d(\alpha z)=\alpha dz$. 追踪上述交换图表, 有 $(\lambda\circ\psi\circ\phi)^*\omega=\alpha\omega$. 记 $\sim$ 表示模 $\mathfrak{P}$ 的约化. 因 E/L 的方程在 $\mathfrak{P}$ 处极小, 于是模 $\mathfrak{P}$ 就得到 $\widetilde{E}$ 的一个方程, 从而约化的微分 $\widetilde{\omega}=\frac{dx}{2y+\widetilde{a}_1x+\widetilde{a}_3}$ 是 $\widetilde{E}$ 上的一个非零微分. 因 $(\alpha)=\mathfrak{a}\mathfrak{p}$ 且 $\mathfrak{P}|\mathfrak{p}$, 有

$$(\widetilde{\lambda}\circ\widetilde{\psi}\circ\widetilde{\phi})^*\widetilde{\omega}=(\widetilde{\lambda\circ\psi\circ\phi})^*\omega=\widetilde{\alpha}\widetilde{\omega}=\widetilde{0}.$$

因此由命题 3.6 知 $\widetilde{\lambda}\circ\widetilde{\psi}\circ\widetilde{\phi}$ 是不可分的. 另一方面, 由引理 4.3 知

$$\begin{aligned}
\deg\widetilde{\phi}&=\deg\phi=N_{K/\mathbb{Q}}(\mathfrak{p})=p,\\
\deg\widetilde{\psi}&=\deg\psi=N_{K/\mathbb{Q}}(\mathfrak{a}),\\
\deg\widetilde{\lambda}&=\deg\lambda=1.
\end{aligned}$$

因 $N_{K/\mathbb{Q}}(\mathfrak{a})$ 与 p 互素, 故 $\widetilde{\psi}$ 和 $\widetilde{\lambda}$ 是可分的, 从而 $\widetilde{\phi}$： $\widetilde{E}\to\widetilde{\overline{\mathfrak{p}}\star E}$ 不可分. 但任何映射均可分解为一个 q 次幂 Frobenius 和一个可分映射之积. 于是 $\deg\widetilde{\phi}=p$ 和 $\widetilde{\phi}$ 的不可分性表明 $\widetilde{\phi}$ 必为 p 次幂 Frobenius 映射. 即存在一个从 $\widetilde{E}^{(p)}$ 到 $\widetilde{\overline{\mathfrak{p}}\star E}$ 的同构, 使得复合

$$\widetilde{E}\ \xrightarrow[\text{Frobenius}]{p\text{ 次幂}}\ \widetilde{E}^{(p)}\ \xrightarrow{\ \sim\ }\ \widetilde{\overline{\mathfrak{p}}\star E}$$

等于 $\widetilde{\phi}$. 特别地有 $j\big(\widetilde{\overline{\mathfrak{p}}\star E}\big)=j\big(\widetilde{E}^{(p)}\big)=j(\widetilde{E})^p$, 从而

$$\begin{aligned}
j(\overline{\mathfrak{p}}\star E)&\equiv j(E)^p=j(E)^{N_{K/\mathbb{Q}}(\mathfrak{p})}\equiv j(E)^{\sigma_\mathfrak{p}}\\
&=j(E^{\sigma_\mathfrak{p}})=j\big(\psi(\sigma_\mathfrak{p})\star E\big)\quad(\bmod\ \mathfrak{P}),
\end{aligned}$$

因此 $\overline{\mathfrak{p}} \star E \cong \psi(\sigma_{\mathfrak{p}}) \star E$. 而 $CL(R_K)$ 在 $EC(R_K)$ 上作用的单性表明 $\psi(\sigma_{\mathfrak{p}}) = \overline{\mathfrak{p}}$. 命题得证.

现在, 我们可以证明这一节的主要结果了.

定理 4.5 设 E 是一条椭圆曲线, 它代表 $EC(R_K)$ 中一个同构类, 则

(a) $K\big(j(E)\big)$ 是 K 的 Hilbert 类域 H;

(b) $[\mathbb{Q}\big(j(E)\big):\mathbb{Q}] = [K\big(j(E)\big):K] = h(K)$, 此处

$$h(K) = \#CL(R_K) = \#\mathrm{Gal}(H/K)$$

是 K 的类数;

(c) 设 $E_1, \cdots, E_h$ 是 $EC(R_K)$ 中一个完全代表元集, 则 $j(E_1), \cdots, j(E_h)$ 是 $j(E)$ 的 $\mathrm{Gal}(\overline{K}/K)$ 共轭类的一个完全集.

(d) 对 K 的每个素理想 $\mathfrak{p}$, 有

$$j(E)^{\sigma_{\mathfrak{p}}} = j\big(\overline{\mathfrak{p}} \star E\big).$$

更一般地, 对每一个非零分式理想 $\mathfrak{A} \subset K$, 有

$$j(E)^{(\mathfrak{A}, H/K)} = j(\overline{\mathfrak{A}} \star E),$$

此处 $(\mathfrak{A}, H/K)$ 是 Artin 映射.

证明 令 L 是同态 ψ: $\mathrm{Gal}(\overline{K}/K) \to CL(R_K)$ 的核的固定域, 则 L/K 是一个有限扩张. 且有

$$\begin{aligned}
\mathrm{Gal}(\overline{K}/L) &= \mathrm{Ker}\psi = \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, \psi(\sigma) = 1\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, \psi(\sigma) \star E = E\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, E^{\sigma} = E\} \ (\psi \text{ 的定义}) \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, j(E^{\sigma}) = j(E)\} \\
&= \{\sigma \in \mathrm{Gal}(\overline{K}/K) \,|\, j(E)^{\sigma} = j(E)\} \\
&= \mathrm{Gal}\big(\overline{K}/K(j(E))\big),
\end{aligned}$$

因此 $L = K\big(j(E)\big)$. 又因为 ψ 将 $\mathrm{Gal}(L/K)$ 单射到 $CL(R_K)$, 故 L/K 是 Abel 扩张, 从而 $L = K\big(j(E)\big)$ 是 K 的一个 Abel 扩张. 为了完成定理 4.5 的证明, 需要类域论中的一些结果.

下面回顾一下类域论中的一些结果, 设 C 是 K 的一个整理想, 它被 L/K 中所有分歧素理想整除. 置

$$I(C) = K \text{ 中与 } C \text{ 互素的分式理想的群},$$

则定义 Artin 映射如下：

$$(\cdot, L/K): I(C) \to \mathrm{Gal}(L/K),$$
$$(\mathfrak{A}, L/K) = \left(\prod_{\mathfrak{p}} \mathfrak{p}^{n_\mathfrak{p}}, L/K\right) = \prod_{\mathfrak{p}} \sigma_\mathfrak{p}^{n_\mathfrak{p}}.$$

定理 4.6 (Artin 互反律) 设 L/K 是数域的有限 Abel 扩张, 则存在一个整理想 $C \subset R_K$, 它正好被 K 中的在 L 中分歧的那些素理想整除, 使得

$$\big((\alpha), L/K\big) = 1, \quad \forall \alpha \in K^*, \alpha \equiv 1 \pmod{C}.$$

注意, 若定理 4.6 对 C_1 和 C_2 成立, 则对 $C_1 + C_2$ 亦然, 因此存在一个最大理想 $C_{L/K}$, 使得定理 4.6 成立. 称 $C_{L/K}$ 是 L/K 的导子 (Conductor). 定义

$$P(C) = \{(\alpha) \mid \alpha \in K^*, \alpha \equiv 1 \pmod{C}\}.$$

由 Artin 互反律, 有

$$\mathfrak{A} \in P(C_{L/K}) \Rightarrow (\mathfrak{A}, L/K) = 1.$$

设 $\mathfrak{p}$ 是 K 的素理想, $\mathfrak{p}$ 在 L 中非分歧, 则 $\mathfrak{p}$ 在 L 中完全分裂当且仅当剩余类域的扩张次数为 1, 或者等价地说, 当且仅当 $(\mathfrak{p}, L/K) = 1$, 因此在 Artin 映射的核中的非分歧素理想正好是 K 在 L 中完全分裂的素理想.

设 C 是 K 的一个整理想, K 模 C 的射类域是一个有限 Abel 扩张 K_C/K, 使得对任意有限 Abel 扩张 L/K, 有

$$C_{L/K} | C \Rightarrow L \subset K_C.$$

定理 4.7 (类域论) 设 L/K 是数域的有限 Abel 扩张, C 是 K 的一个整理想, 则

(a) Artin 映射

$$(\cdot, L/K): \ I(C_{L/K}) \to \mathrm{Gal}(L/K)$$

是满同态.

(b) Artin 映射的核是 $(N_{L/K} I_L) P(C_{L/K})$, I_L 是 L 的非零分式理想的群.

(c) 存在惟一的一个模 C 的射类域 K_C, K_C/K 的导子整除 C.

(d) 射类域 K_C 由下述性质刻画：它是 K 的一个 Abel 扩张且满足

$$\{K\text{的在 } K_C \text{ 中完全分裂的素理想}\} = \{P(C)\text{中的素理想}\}.$$

如果 $C=(1)$, 则 K 模 $C=(1)$ 的射类域是 K 的极大 Abel 非分歧扩张, 称之为 K 的 Hilbert 类域, 记为 H_K 或 H, 此时

$$I(C_{H/K})=I\big((1)\big)=\{K\text{的所有非零分式理想}\},$$
$$P(C_{H/K})=P\big((1)\big)=\{K\text{的所有非零主理想}\},$$

于是 Artin 映射诱导出 K 的理想类群和 K 的 Hilbert 类域的 Galois 群之间的同构

$$(\cdot,H/K):\ CL(R_K)\longrightarrow \mathrm{Gal}(H/K).$$

最后, 叙述 Dirichlet 素数定理.

定理 4.8 *设 K 为数域, C 为 K 的一个整理想, 则在 $I(C)/P(C)$ 的每个理想类中存在无穷多个次数为 1 的 K 的素理想.*

证明 [定理 4.5 的证明 (继续)] 令 $C_{L/K}$ 是 L/K 的导子, 其中 $L=K\big(j(E)\big)$. 考虑 Artin 映射与 ψ 的复合

$$I(C_{L/K})\xrightarrow{(\cdot,L/K)}\mathrm{Gal}(L/K)\xrightarrow{\ \psi\ }CL(R_K).$$

我们将证明下述事实:

$$\psi\big((\mathfrak{A},L/K)\big)=\overline{\mathfrak{A}},\ \forall\mathfrak{A}\in I(C_{L/K}). \tag{4.12}$$

设 $\mathfrak{A}\in I(C_{L/K})$, S 是命题 4.1 中的有理素数的有限集. 由定理 4.8, 存在一个次数为 1 的素理想 $\mathfrak{p}\in I(C_{L/K})$, 使得 $\mathfrak{A}$ 与 $\mathfrak{p}$ 在同一个 $P(C_{L/K})$ 理想类中, 且不位在 S 的素数上. 换言之, 存在 $\alpha\in K^*$, 使得

$$\alpha\equiv 1\pmod{C_{L/K}}\ \text{且}\ \mathfrak{A}=(\alpha)\mathfrak{p}.$$

于是

$$\begin{aligned}\psi\big((\mathfrak{A},L/K)\big)&=\psi\big(((\alpha)\mathfrak{p},L/K)\big)\ (\text{因}\mathfrak{A}=(\alpha)\mathfrak{p})\\&=\psi\big((\mathfrak{p},L/K)\big)\ (\text{因}\alpha\equiv 1\pmod{C_{L/K}})\\&=\psi(\sigma_{\mathfrak{p}})\qquad(\text{Artin 映射的定义})\\&=\overline{\mathfrak{p}}\qquad(\text{命题 4.1})\\&=\overline{\mathfrak{A}}\qquad(\text{因}\mathfrak{A}=(\alpha)\mathfrak{p}).\end{aligned}$$

这就证明了上述"事实".

作为 (4.12) 式的一个结果, 显然有

$$\psi\big((\alpha),L/K\big)=1,\ \forall\ \text{主理想}\ (\alpha\in I(C_{L/K})).$$

又因为 ψ: $\mathrm{Gal}(L/K) \to CL(R_K)$ 是单的, 故

$$\big((\alpha), L/K\big) = 1, \quad \forall (\alpha) \in I(C_{L/K}).$$

但 L/K 的导子是具有下述性质的最小整理想 C:

$$\alpha \equiv 1 \pmod{C} \Longrightarrow \big((\alpha), L/K\big) = 1,$$

于是知 $C_{L/K} = (1)$. 但导子被每一个分歧素理想整除, 于是由 $C_{L/K} = (1)$ 知 L/K 是无处分歧的, 从而 L 包含在 K 的 Hilbert 类域 H 之中.

另一方面, 自然映射 $I(C_{L/K}) = I\big((1)\big) \to CL(R_K)$ 显然是满的, 故 (4.12) 式表明 ψ: $\mathrm{Gal}(L/K) \to CL(R_K)$ 是满的, 从而是一个同构, 故

$$[L:K] = \#\mathrm{Gal}(L/K) = \#CL(R_K) = \#\mathrm{Gal}(H/K) = [H:K].$$

再由 $L \subset H$ 知 $L = H$. 这就完成了 (a) 的证明 (因 $L = K\big(j(E)\big)$).

(b) 由于定理 4.3(b) 有 $[\mathbb{Q}(j(E)) : \mathbb{Q}] \leqslant h(K)$, 但刚才我们证明了 $[K(j(E)) : K] = h(K)$, 所以有

$$\big[K\big(j(E)\big) : \mathbb{Q}\big] = \big[K\big(j(E)\big) : K\big]\big[K : \mathbb{Q}\big] = 2h(K),$$
$$\big[K\big(j(E)\big) : \mathbb{Q}\big] = \big[K\big(j(E)\big) : \mathbb{Q}\big(j(E)\big)\big]\big[\mathbb{Q}\big(j(E)\big) : \mathbb{Q}\big] = 2h(K),$$

从而 $\big[\mathbb{Q}\big(j(E)\big) : \mathbb{Q}\big] = 2h(K)/\big[K\big(j(E)\big) : \mathbb{Q}\big(j(E)\big)\big] \geqslant h(K)$. 于是

$$\big[\mathbb{Q}\big(j(E)\big) : \mathbb{Q}\big] = h(K),$$

其中用到了 $\big[K\big(j(E)\big) : \mathbb{Q}\big(j(E)\big)\big] \leqslant 2$ (因为 $[K:\mathbb{Q}] = 2$).

(c) 由定理 4.2(b), $CL(R_K)$ 传递地作用在 j 不变量的集合

$$J = \{j(E_1), \cdots, j(E_h)\}$$

上. 而由映射 ψ: $\mathrm{Gal}(\overline{K}/K) \to CL(R_K)$ 的定义知

$$E_i^{\sigma} = \psi(\sigma) \star E_i, \ \forall \sigma \in \mathrm{Gal}(\overline{K}/K), \ E_i \in EC(R_K),$$

且

$$j(E_i)^{\sigma} = j\big(E_i^{\sigma}\big) = j\big(\psi(\sigma) \star E_i\big),$$

可见 $\mathrm{Gal}(\overline{K}/K)$ 也传递作用在 J 上, 从而 J 是 $j(E)$ 的 $\mathrm{Gal}(\overline{K}/K)$ 共轭的完全集.

(d) (4.12) 式表明 (d) 对所有 $I(C_{L/K})$ 中理想均成立. 但 $C_{L/K} = (1)$, 故 $I(C_{L/K})$ 就是 K 中所有非零分式理想的集合, 于是定理得证.

下面的目的是要找出具有复乘 R_K 的椭圆曲线 E 的 j 不变量 $j(E)$ 的极小多项式. 由定理 4.5, 我们知道它应该是 $h(K)$ 次的. 为此目的, 需要讨论虚二次域的理想与正定二元二次型之间的关系.

设 $D<0$ 是无平方因子的有理整数, 则 $\mathbb{Q}(\sqrt{D})$ 的判别式为 $\Delta=D$ 或 $4D$(按 $D\equiv 1 \pmod 4$ 或 $D\equiv 2,3 \pmod 4$), 设 $\mathfrak{a}$ 为 $\mathbb{Q}(\sqrt{D})$ 之整理想, α_1,α_2 是 $\mathfrak{a}$ 的一组 $\mathbb{Z}$ 基, 且适合

$$\alpha_1\alpha_2'-\alpha_1'\alpha_2=N(\mathfrak{a})\sqrt{\Delta}, \tag{4.13}$$

此处 α_i' 是 α_i 的共轭数, $N(\mathfrak{a})$ 表示理想的范数. 于是可得一个二次型

$$\begin{aligned}F(x,y)&=N(\alpha_1x+\alpha_2y)/N(\mathfrak{a})=((\alpha_1x+\alpha_2y)(\alpha_1'x+\alpha_2'y))/N(\mathfrak{a})\\&=ax^2+bxy+cy^2.\end{aligned}$$

因 $\alpha_1,\alpha_2,\alpha_1+\alpha_2\in\mathfrak{a}$, 故 $a=N(\alpha_1)/N(\mathfrak{a})$, $b=(N(\alpha_1x+\alpha_2y)-N(\alpha_1)-N(\alpha_2))/N(\mathfrak{a})$ 和 $c=N(\alpha_2)/N(\mathfrak{a})$ 均为有理整数, 而 $F(x,y)$ 的判别式为

$$b^2-4ac=\left((\alpha_1\alpha_2'-\alpha_1'\alpha_2)/N(\mathfrak{a})\right)^2=\Delta,$$

故 $F(x,y)$ 为判别式等于 Δ 的正定二元二次型. 称 $F(x,y)$ 为伴随到 $\mathfrak{a}$ 的二次型.

反之, 若

$$F(x,y)=ax^2+bxy+cy^2$$

是判别式为 Δ 的正定二次型, 则令 $\mathfrak{a}$ 是 a 和 $\frac{b-\sqrt{\Delta}}{2}$ 生成的理想

$$\mathfrak{a}=\left(a,\frac{b-\sqrt{\Delta}}{2}\right),$$

易知 $\mathfrak{a}$ 具有一组 $\mathbb{Z}$ 基 $\left\{a,\frac{b-\sqrt{\Delta}}{2}\right\}$. 直接计算知 $N(\mathfrak{a})=a$, 而对应于 $\mathfrak{a}$ 的二次型为

$$\frac{\left(ax+\frac{1}{2}(b-\sqrt{\Delta})y\right)\left(ax+\frac{1}{2}(b+\sqrt{\Delta})y\right)}{a}=ax^2+bxy+cy^2.$$

不难验证下面的结论:

定理 4.9 上述适合 (4.13) 式的理想与二次型之间的映射诱导出理想类群和相似二次型类之间的一个一一对应. 即: 若 $\mathfrak{a}_1$ 和 $\mathfrak{a}_2$ 是 $\mathbb{Q}(\sqrt{D})$ 中适合 (4.13) 式的整理想, 则 $\mathfrak{a}_1$ 和 $\mathfrak{a}_2$ 在同一个理想类中当且仅当伴随到 $\mathfrak{a}_1$ 和 $\mathfrak{a}_2$ 的二次型是相似的 (二次型 $F(x,y)$ 与 $G(x,y)$ 称为相似的, 如果存在整数 q,r,s,t, 使得 $F(qx+ry,sx+ty)=G(x,y)$ 且 $qt-rs=1$. 记为 $F(x,y)\sim G(x,y)$).

于是我们自然地考虑判别式为 Δ 的所有正定二元二次型在相似下的等价类的代表元的完全集, 这就是

定理 4.10 判别式为 d 的正定二元二次型的类数等于适合

$$b^2 - 4ac = d, \text{ 且 } -a < b \leqslant a < c \text{ 或 } 0 \leqslant b \leqslant a = c \tag{4.14}$$

的整数组 a, b, c 的数目.

证明 首先证明任意一个相似类中一定有一个二次型$\{a,b,c\}$满足定理中条件.

设 k 为任意一个相似类, 而 a 是 k 所能表示的最小正整数, 再令 $\{a_0, b_0, c_0\}$ 为 k 中任意一个二次型, 则存在 r, t, 使得

$$a = a_0r^2 + b_0rt + c_0t^2, \text{ 且 } (r,t) = 1$$

(否则, $\frac{a}{(r,t)^2}$ 也可由 $\{a_0, b_0, c_0\}$ 表示, 而 $\frac{a}{(r,t)^2} < a$ 矛盾). 选取 s, u, 使得 $ru - st = 1$, 则 $\{a_0, b_0, c_0\}$ 经 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ 变为 $\{a, b', c'\}$, 而 $\{a, b', c'\}$ 经过 $\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}$ 变为 $\{a, b, c\}$, 其中 $b = 2ah + b'$. 我们总可以取整数 h, 使得 $|b| \leqslant a$. 但 c 可由 $\{a, b, c\}$ 表出, 而 $\{a, b, c\}$ 与 $\{a_0, b_0, c_0\}$ 均属于 k, 故 $a \leqslant c$, 从而知 k 中至少有一个二次型适合 $-a \leqslant b \leqslant a \leqslant c$. 但

$$\{a, -a, c\} \sim \{a, a, c\}$$

(因 $\{a, -a, c\}$ 经 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ 变为 $\{a, a, c\}$), 且

$$\{a, -b, a\} \sim \{a, b, a\}$$

(因 $\{a, -b, a\}$ 经 $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ 变为 $\{a, b, a\}$), 故 k 中一定存在二次型 $\{a, b, c\}$ 满足定理中的条件.

其次, 证明定理中所列出之二次型不相似. 即若 $\{a, b, c\} \sim \{a', b', c'\}$ 且都适合 (4.14) 式, 则 $a = a', b = b', c = c'$.

不妨设 $a' \leqslant a$. 令 $\begin{pmatrix} r & s \\ t & u \end{pmatrix}$ 将 $\{a, b, c\}$ 变为 $\{a', b', c'\}$, 则

$$a' = ar^2 + brt + ct^2, \tag{4.15}$$

$$b' = 2ars + b(ru + st) + 2ctu. \tag{4.16}$$

由 (4.15) 式知

$$a \geqslant a' \geqslant ar^2 - a|rt| + at^2 = a\big(|r| - |t|\big)^2 + a|rt| \geqslant a|rt|, \tag{4.17}$$

即 $|rt| \leqslant 1$. 若 $|rt| = 1$, 则 $a = a'$. 若不然, 则 $rt = 0$, 此时

$$a \geqslant a' \geqslant ar^2 + at^2 = a(r^2 + t^2) \geqslant a,$$

也有 $a = a'$.

下设 $c > a$, 则 t 必为 0, 若不然, 由 (4.15) 式及 $|rt| \leqslant 1$ 和 $|b| \leqslant a$ 知, $a \geqslant a' = ar^2 + brt + ct^2 \geqslant ct^2 > c$, 矛盾, 故 $t = 0$, $ru = 1$. 由 (4.16) 式,

$$b' = 2ars + b \equiv b \pmod{2a},$$

因 $-a < b \leqslant a$ 及 $-a = -a' < b' \leqslant a' = a$, 可知 $b' = b$, 由此立得 $c = c'$. 若 $c' > a'(= a)$, 可类似证明. 最后, 设 $a = a' = c = c'$, 此时必有 $b = \pm b'$, 但 $b \geqslant 0$, $b' \geqslant 0$, 故 $b = b'$, 证毕.

称满足 (4.14) 式的一个正定二次型为既约二次型. 由定理 4.5 和 4.9 及 4.10, 立即有下面的结果:

定理 4.11 设 $\tau \in \mathfrak{H}$ 是判别式为 $-D < 0$ 的一个复二次数, 即 $(\tau, 1)$ 满足一个判别式为 $-D$ 的本原正定二次型 $Q(x, y)$ (即 $Q(\tau, 1) = 0$), 则 $j(\tau)$ 是一个次数为 $h(D)$ 的代数整数, 其极小多项式为

$$H_D(x) = \prod \big(x - j(\alpha)\big),$$

其中 α 是所有可能的复数, 使得 $(\alpha, 1)$ 是某个判别式为 $-D$ 的本原既约二次型的零点, 其中一个二次型 $\{a, b, c\}$ 称为本原的, 如果 $(a, b, c) = 1$.

$H_D(x)$ 称为判别式为 $-D$ 的 Hilbert 类多项式. 为了计算 $H_D(x)$, 需要计算 $j(\tau)$ 的值 ($\tau \in \mathfrak{H}$), 这可以利用下面的公式来进行计算:

$$j(\tau) = \frac{\big(256h(\tau) + 1\big)^3}{h(\tau)}, \quad h(\tau) = \frac{\Delta(2\tau)}{\Delta(\tau)},$$

$$\Delta(\tau) = q\prod_{n=1}^{\infty}(1 - q^n)^{24} = q\Big(1 + \sum_{n\geqslant 1}(-1)^n\big(q^{n(3n-1)/2} + q^{n(3n+1)/2}\big)\Big)^{24},$$

此处 $q = e^{2\pi i\tau}$, 于是 $H_D(x)$ 可以通过计算 $j(\alpha)$ 的值并计算乘积

$$H_D(x) = \prod_{\alpha}\big(x - j(\alpha)\big)$$

而得出, 其中的乘积跑遍所有形式如下的数:

$$\alpha = \big(-b + \sqrt{-D}\big)/(2a),$$

其中 $b^2 - 4ac = -D$, 而 $ax^2 + bxy + cy^2$ 是判别式为 $-D$ 的本原既约正定二元二次型.

§4.2　利用复乘生成椭圆曲线

我们的目的是要探讨有限域 $\mathbb{F}_q$(其中$q=p^n$) 上具有复乘的椭圆曲线的性质. 下面的定理给出了有限域上具有复乘的椭圆曲线与复数域上具有复乘的椭圆曲线之间的关系：

定理 4.12　设 K 是一个虚二次域, R_K 是其整数环, 而 $E/\overline{\mathbb{Q}}$ 是具有复乘 R_K 的一条椭圆曲线. 对于任意有理素数 p, 设 $\mathfrak{P}$ 是 $\overline{\mathbb{Q}}$ 的一个位于 p 上的素理想, 使得 E 具有非退化的模 $\mathfrak{P}$ 的约化 $\widetilde{E}$, 则 $\widetilde{E}$ 是超奇异的当且仅当 p 在 K 中仅有一个位于其上的素理想 (即 p 在 K 中是分歧的或仍为素的). 若 p 在 K 中完全分裂, 则自然映射

$$M:\quad \mathrm{End}(E)\longrightarrow \mathrm{End}(\widetilde{E})$$
$$\psi\longmapsto\widetilde{\psi}$$

是一个同构.

证明　首先假定定理 4.12 的前半部分已经证得, 于是当 p 在 K 中完全分裂时, $\widetilde{E}$ 不是超奇异的, 于是 $\widetilde{E}$ 的自同态环必为虚二次域 K 中的一个阶. 但引理 4.3 表明 M 是一个单射, 于是 $\mathrm{End}(E)=R_K\longrightarrow\mathrm{End}(\widetilde{E})$. 但 R_K 是 K 中的最大阶, 从而 $\mathrm{End}(\widetilde{E})=R_K$, 进而 M 是一个同构.

下面证明定理的前半部分. 首先证明：若 p 在 K 中完全分裂, 则 $\widetilde{E}$ 不是超奇异的. 设 $pR_K=\mathfrak{p}\mathfrak{p}'$, $\mathfrak{p}\neq\mathfrak{p}'$, 且 $\mathfrak{P}\cap R_K=\mathfrak{p}$. 只要证明 $\widetilde{E}$ 具有阶数为 p 的点即可. 记

$$\theta:\ R_K\longrightarrow\mathrm{End}(E)$$

是引理 4.2 的正规化嵌入 $[\cdot]$, 于是 $\theta(R_K)=\mathrm{End}(E)$. 令 m 是一个正整数, 使得 $\mathfrak{p}^m$ 和 $\mathfrak{p}'^m$ 是主理想

$$\mathfrak{p}^m=\mu R_K,\quad \mathfrak{p}'^m=\mu' R_K,$$

则 $\overline{\mu\mu'}=p^m$. 注意到 $\mu'\notin\mathfrak{p}$ 且 θ 是正规化嵌入, 从而对 E 上的任意的不变微分 ω, $\mu'\omega$ 模 $\mathfrak{P}$ 约化是非零的 (因为 $\mu'\not\equiv 0 \pmod{\mathfrak{P}}$), 故 $\overline{\mu'\omega}\equiv\overline{\mu'}\overline{\omega}\not\equiv 0 \pmod{\mathfrak{P}}$, 从而 $\overline{\theta(\mu')}$ 是可分的. 但 $\mu\mu'=p^m$ 表明 $\theta(\mu')$ 的次数是 p 的一个幂次, 从而其模 $\mathfrak{P}$ 的约化次数亦然, 进而 $\widetilde{E}$ 具有非平凡的 p 阶点, 于是 $\widetilde{E}$ 不是超奇异的.

其次, 我们证明：若 p 在 K 中不是完全分裂的, 则 $\widetilde{E}$ 必为超奇异的. 事实上, 设 $pR_K=\mathfrak{p}^m$, 由下面将要证明的引理 4.4, 存在一个元素 $\mu\in R_K$, 使得 $\theta(\mu)$ 模 $\mathfrak{p}$ 约化到一个 Frobenius 自同态. 因为 $pR_K=\mathfrak{p}^m$, 又因为 $\mu\mu'$ 是 p 的一个幂次 (μ' 记 μ 在 K 中的共轭), 从而 μ' 与 μ 仅相差 R_K 中一个单位, 从而 $\theta(\mu)\theta(\mu')=q\sigma$, 其中 q 为 p 的一个幂次, σ 是 E 的自同构, 这意味着 $q\sigma$ 是 $\widetilde{E}$ 上纯不可分的, 从而 $\widetilde{E}$ 是超奇异的, 证毕.

引理 4.4 设 K 是一个虚二次域, H 是 K 的 Hilbert 类域, E/H 是具有复乘 R_K 的椭圆曲线, 则除掉有限个外, 对 K 中次数为 1 且满足 $(\mathfrak{p}, H/K)=1$ 的素理想 $\mathfrak{p}$, 存在惟一的元素 $\pi=\pi_{\mathfrak{p}}\in R_K$, 使得 $\mathfrak{p}=\pi R_K$, 且

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow{\phi:\, p\text{ 次 Frobenius}} & \widetilde{E} \end{array}$$

是交换的.

证明 由命题 4.1 的证明过程, 存在 K 的有限个次数为 1 的素理想组成的集合 S, 使得对任意次数为 1 的素理想 $\mathfrak{p}\notin S$, 自然映射

$$E \longrightarrow \overline{\mathfrak{p}}\star E \tag{4.18}$$

的次数均为 p, 且其约化 $\widetilde{E}\longrightarrow\widetilde{\overline{\mathfrak{p}}\star E}$ 是纯不可分的, 其中约化是模 $\mathfrak{P}\subset H$ 的, $\mathfrak{P}|\mathfrak{p}$. 记 $\sigma=\sigma_{\mathfrak{p}}$ 是对应于 $\mathfrak{p}$ 的 Frobenius, 将 (4.18) 式复合上定理 4.5 中的同构 $\overline{\mathfrak{p}}\star E\cong E^{\sigma}$, 得到一个同种 $\widetilde{\lambda}$: $\widetilde{E}\longrightarrow E^{\sigma}$, 它是次数 p 的纯不可分的同种. 于是 $\widetilde{\lambda}$ 分解如下:

$$\widetilde{E}\xrightarrow{\phi}\widetilde{E}^{(p)}\xrightarrow{\varepsilon}\widetilde{E^{\sigma}},$$

此处 ϕ 是 p 次幂 Frobenius 映射而 $\deg\varepsilon=1$. 但是, 由定义, E^{σ} 的约化正好是 $\widetilde{E}^{(p)}$, 故 ε 是 $\widetilde{E^{\sigma}}$ 的一个同构. 若能证明 ε 是某个 $\varepsilon_0\in\mathrm{Aut}(E^{\sigma})$ 的模 $\mathfrak{P}$ 的约化, 则可以用 $\varepsilon_0^{-1}\circ\lambda$ 替代 λ, 从而获得下述交换图表:

$$\begin{array}{ccc} E & \xrightarrow{\lambda} & E^{\sigma_{\mathfrak{p}}} \\ \downarrow{\scriptstyle \bmod \mathfrak{P}} & & \downarrow{\scriptstyle \bmod \mathfrak{P}} \\ \widetilde{E} & \xrightarrow{p\text{ 次 Frobenius}} & \widetilde{E}^{(p)} \end{array} \tag{4.19}$$

现在假定 (4.19) 式由于 $(\mathfrak{p}, H/K)=1$, 故 $E^{\sigma_{\mathfrak{p}}}=E$, 从而 $\widetilde{E}^{(p)}=\widetilde{E}$, 因此 λ 是 E 的一个自同态, 于是 $\lambda\in\mathrm{End}(E)=R_K$. 设 $\lambda=[\pi]$, 故有交换图表

$$\begin{array}{ccc} E & \xrightarrow{[\pi]} & E \\ \downarrow & & \downarrow \\ \widetilde{E} & \xrightarrow[p\text{ 次 Frobenius}]{\phi:} & \widetilde{E} \end{array} \tag{4.20}$$

因为 $\mathfrak{p}$ 的次数为 1, 且 $\widetilde{[\pi]}=\phi$, 由引理 4.3, 有

$$N_{K/\mathbb{Q}}(\mathfrak{p})=p=\deg(\mathfrak{p})=\deg[\pi]=|N_{K/\mathbb{Q}}(\pi)|.$$

但 $\mathfrak{p}$ 是虚二次域 K 中素理想, 上述等式意味着

$$\mathfrak{p} = \pi R_K \text{ 或 } \mathfrak{p} = \pi' R_K,$$

此处 π' 是 π 的 $\mathrm{Gal}(K/\mathbb{Q})$ 共轭.

取 E/H 的一个方程, 使它在 $\mathfrak{P}$ 有好约化, 令 $\omega \in \Omega_E$ 是一个非零不变微分, 使得其约化 $\widetilde{\omega}$ 是 $\widetilde{E}$ 上的一个非零不变微分. 于是引理 4.2 中的正规化映射表明 $[\pi]^*\omega = \pi\omega$, 从而

$$\widetilde{\pi}\widetilde{\omega} = \widetilde{\pi\omega} = \widetilde{[\pi]^*\omega} = \widetilde{[\pi]}^*\widetilde{\omega} = \phi^*\widetilde{\omega} = 0.$$

这里用到了 (4.20) 是一个交换图及 ϕ 的不可分性 (从而 $\phi^*\widetilde{\omega} = 0$). 但 $\Omega_{\widetilde{E}}$ 是由 $\widetilde{\omega}$ 生成的 1 维向量空间, 从而 $\widetilde{\pi} = 0$, 即 $\pi \in \mathfrak{P}$, 于是 $\pi \in \mathfrak{P} \cap K = \mathfrak{p}$, 故 $\mathfrak{p} = \pi R_K$. 这就证明了引理 4.4 的存在部分.

为了说明 π 的惟一性, 我们只要注意到下述复合映射是单的:

$$R_K \xrightarrow{[\cdot]} \mathrm{End}(E) \longrightarrow \mathrm{End}(\widetilde{E}),$$

因为 π 要满足 $\widetilde{[\pi]} = \phi \in \mathrm{End}(\widetilde{\phi})$, 故由上式映射的单性, 知这样的 π 最多只有一个. 于是只要能证明 (4.19) 式, 就可以得出引理 4.4 的证明, 这就是下面的

引理 4.5 *设 K 是一个虚二次域, H 是 K 的 Hilbert 类域, E/H 是具有复乘 R_K 的椭圆曲线, 设 $\sigma = \sigma_{\mathfrak{p}} \in \mathrm{Gal}(H/K)$ 是伴随到 R_K 的一个素理想 $\mathfrak{p}$ 的 Frobenius 元, $\mathfrak{P}$ 是 H 中位于 $\mathfrak{p}$ 上的一个素理想. 假定 $\mathfrak{p}$ 具有次数 1 且 $\mathfrak{p} \notin S$ (S 如引理 4.4 证明开始时所述), 从而 E 在 $\mathfrak{P}$ 处有好的约化, 则存在一个同种 λ: $E \longrightarrow E^{\sigma_{\mathfrak{p}}}$, 使得 λ 模 $\mathfrak{P}$ 的约化是 p 次幂 Frobenius, 即 (4.19) 是交换图表.*

证明 记号与引理 4.4 证明中相同. 由引理 4.4 的证明, 仅需要证明 ε 是某个 $\varepsilon_0 \in \mathrm{Aut}(E^\sigma)$ 模 $\mathfrak{P}$ 的约化. 也就是说, $\varepsilon \in \theta(\mathrm{Aut}(E^\sigma))$, 其中 θ 是引理 4.3 中的自然同态. 为此, 首先证明 ε 与 $\theta\big(\mathrm{End}(E^\sigma)\big)$ 中任意元可交换. 回顾我们有正规化同构如下:

$$[\cdot]_E: \ R_K \cong \mathrm{End}(E), \quad [\cdot]_{E^\sigma}: \ R_K \cong \mathrm{End}(E^\sigma),$$

它具有以下性质:

$$\begin{aligned} &\Psi \circ [\alpha]_E = [\alpha]_E \circ \Psi, \quad \forall \Psi \in \mathrm{End}(E, E^\sigma), \forall \alpha \in R_K, \\ &[\alpha]_E^\sigma = [\alpha]_{E^\sigma} \ (\text{引理 } 4.2(\mathrm{b})). \end{aligned} \tag{4.21}$$

记 ϕ 是 p 次幂 Frobenius, 则易知有

$$\phi \circ \widetilde{[\alpha]_E} = \widetilde{[\alpha]_E^\sigma} \circ \phi = \widetilde{[\alpha]}_{E^\sigma} \circ \phi \tag{4.22}$$

(事实上, 对任意定义在特征 p 的域 k 上的代数簇 V 和 W 之间的有理映射 f, 易知有 $\phi_W \circ f = f^\sigma \circ \phi_V$, 其中 $\sigma \in \mathrm{Aut}(k)$ 是 p 次幂 Frobenius 自同构, ϕ_V 和 ϕ_W 分别是 V 和 W 上的 p 次幂 Frobenius 映射). 于是有

$$\begin{aligned}\widetilde{[\alpha]}_{E^\sigma} \circ \varepsilon \circ \phi &= \widetilde{[\alpha]}_{E^\sigma} \circ \widetilde{\lambda} \ (\text{因为 } \varepsilon \circ \phi = \widetilde{\lambda}) \\ &= \widetilde{\lambda} \circ \widetilde{[\alpha]}_E \qquad (\text{由 (4.21) 式}) \\ &= \varepsilon \circ \phi \circ \widetilde{[\alpha]}_E \\ &= \varepsilon \circ \widetilde{[\alpha]}_{E^\sigma} \circ \phi \qquad (\text{由 (4.22) 式}),\end{aligned}$$

这表明 $\widetilde{[\alpha]}_{E^\sigma} \circ \varepsilon = \varepsilon \circ \widetilde{[\alpha]}_{E^\sigma}$. 可见 ε 与 $\theta(\mathrm{End}(E))$ 中任意元可交换.

其次证明: 一个自同态 $\gamma \in \mathrm{End}(\widetilde{E})$ 是落在 $\mathrm{Im}(\theta) = \theta(\mathrm{End}(E))$ 中, 当且仅当 γ 与 $\mathrm{Im}(\theta)$ 中每一个元素可交换.

必要性是显然的, 这是因为 θ 是单的, 故 $\mathrm{Im}(\theta) \cong \mathrm{End}(E) = R_K$ 是交换环, 从而若 $\gamma \in \mathrm{Im}(\theta)$, 则 γ 当然与 $\mathrm{Im}(\theta)$ 中任意元素可交换.

下证充分性. 因 $\mathrm{End}(\widetilde{E})$ 是一个虚二次域或一个四元数代数中的阶, 故分两种情形讨论. 若 $\mathrm{End}(\widetilde{E})$ 为一个虚二次域中的阶, 则 θ 必为同构 (因由引理 4.3), θ 是单的, 而由假设, $\mathrm{End}(E) = R_K$ 是 K 中的最大阶, 于是 $\theta(\mathrm{End}(E)) = \mathrm{End}(\widetilde{E})$.

下面假设 $\mathrm{End}(\widetilde{E})$ 是四元数代数 $\mathfrak{H}$ 的一个阶, 则 $\mathrm{Im}(\theta) \otimes \mathbb{Q}$ 是 $\mathfrak{H}$ 的一个 2 次子域, 令其为 $\mathcal{K}$. 选取 $\mathcal{K}$ 的一组 $\mathbb{Q}$ 基 $\{1, \alpha\}$, 使得 $\alpha^2 \in \mathbb{Q}$, 将其扩充为 $\mathfrak{H}$ 的一组 $\mathbb{Q}$ 基

$$\mathfrak{H} = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta,$$

使得 $\alpha^2, \beta^2, (\alpha\beta)^2 \in \mathbb{Q}$, $\alpha\beta = -\beta\alpha$. 下面找出 $\mathcal{K}$ 在 $\mathfrak{H}$ 中的交换子. 对任意 $\gamma \in \mathfrak{H}$, 令 $\gamma = d + a\alpha + b\beta + c\alpha\beta$, $a, b, c, d \in \mathbb{Q}$, 则有

$$\begin{aligned}\gamma\text{与}\mathcal{K}\text{中元素交换} &\iff \gamma\alpha = \alpha\gamma \\ &\iff (d + a\alpha + b\beta + c\alpha\beta)\alpha = \alpha(d + a\alpha + b\beta + c\alpha\beta) \\ &\iff -b\alpha\beta - c\alpha^2\beta = b\alpha\beta + c\alpha^2\beta \qquad (\alpha\beta = -\beta\alpha) \\ &\iff b = c = 0 \ (\alpha^2 \in \mathbb{Q}, \text{且 } \{1, \alpha, \beta, \alpha\beta\} \text{ 是 } \mathfrak{H} \text{ 的一组 } \mathbb{Q} \text{ 基}) \\ &\iff \gamma = d + a\alpha \in \mathbb{Q} + \mathbb{Q}\alpha = \mathcal{K}.\end{aligned}$$

现在, 设 $\delta \in \mathrm{End}(\widetilde{E})$ 与 $\mathrm{Im}(\theta)$ 交换, 则 δ 与 $\mathcal{K}$ 交换, 于是由上面的证明, $\delta \in \mathcal{K}$. 但是 δ 在 $\mathbb{Z}$ 上是整的, 且 $\mathrm{Im}(\theta) \cong R_K$ 是 $\mathcal{K} \,(\cong K)$ 中的最大阶, 故 $\delta \in \mathrm{Im}(\theta)$. 这就证明了我们的结论.

结合前面的过程, 知道 $\varepsilon \in \mathrm{Im}(\theta)$, 其中

$$\theta: \ \mathrm{End}(E^\sigma) \to \mathrm{End}(\widetilde{E}^\sigma),$$

即存在 $\varepsilon_0 \in \mathrm{End}(E^\sigma)$, 使得 $\varepsilon = \widetilde{\varepsilon}_0$, 由引理 4.3 知 $\deg \varepsilon_0 = \deg \varepsilon = 1$, 从而 $\varepsilon_0 \in \mathrm{Aut}(E^\sigma)$, 证毕.

由定理 4.12, 若 $\overline{E}/\mathbb{F}_p$ 是有限域 (p 为素数) 上具有复乘 R_K 的椭圆曲线, 且存在椭圆曲线 $E/\overline{\mathbb{Q}}$(具有复乘 R_K), 使得 E 模 $\mathfrak{P}$ 的约化 $\widetilde{E}$ 正好是 $\overline{E}$, 则 p 在 K 中是完全分裂的.

定理 4.13 设 $\overline{E}/\mathbb{F}_q$ 是定义在有限域 $\mathbb{F}_q$ 上的非超奇异椭圆曲线, $q = p^d$, 它具有复乘 R_K, 而 $\pi = \pi_q$ 是其上的 Frobenius 自同态, 则 $\pi \notin \mathbb{Z}$. 又若 $pR_K = \mathfrak{p}\mathfrak{p}'$ 是 p 在 $R_K = \mathrm{End}(\overline{E})$ 中的分解, 则

$$\pi R_K = \mathfrak{p}^d \quad 或 \quad \pi R_K = \mathfrak{p}'^d,$$

且 πR_K 任何其他生成元必为 $\pm\pi$

证明 假设 $\pi \in \mathbb{Z}$, 即 $\pi = [n]$, 对某个 $n \in \mathbb{Z}$, 因 $\deg(\pi) = q$, $\deg([n]) = n^2$, 故 $q = \deg(\pi) = n^2$, 从而 $n = p^m$(对某个整数 m). 但 π 是纯不可分的, 故 π 的核为 0, 从而 $[p^m] = \pi$ 的核为 0, 于是 Tate 模 $T_p = 0$. 即 $\overline{E}$ 是超奇异的, 与定理假设条件矛盾, 故 $\pi \notin \mathbb{Z}$. 现在 $\pi \in R_K \setminus \mathbb{Z}$, 令 π' 是 π 的共轭元, 由于 $\deg(\pi) = q$, 故 $\pi\pi' = q = p^d$, 可见只有 p 的因子能够成为 π 或 π' 的因子. 但 p 不整除 π(因为 π 是纯不可分的, 故其核为 0, 而由 $\overline{E}$ 的非超奇异性知 $[p]$ 具有非平凡的核), 从而 $\mathfrak{p}$ 和 $\mathfrak{p}'$ 不能同时整除 πR_K, 于是适当调整 $\mathfrak{p}$ 和 $\mathfrak{p}'$, 可设 $\pi R_K = \mathfrak{p}^m$, 且 $\pi' R_K = \mathfrak{p}'^m$, 因此 $p^d R_K = \pi\pi' R_K = \mathfrak{p}^m \mathfrak{p}'^m = (\mathfrak{p}\mathfrak{p}')^m = p^m R_K$, 可见 $m = d$. 又因为 $\overline{E}$ 非超奇异, 故 $\overline{E}$ 的自同构只有 ± 1, 因此 π 惟一决定到 ± 1, 证毕.

特别地, 若 $q = p$ 为素数, 则有以下的

推论 4.1 设 $\overline{E}/\mathbb{F}_p$ 是具有复乘 R_K 的椭圆曲线, 则 $\pi \in R_K \setminus \mathbb{Z}$, p 在 R_K 中完全分裂为 $pR_K = \mathfrak{p}\mathfrak{p}'$, 且 $\mathfrak{p} = \pi R_K$, $\mathfrak{p}' = \pi' R_K$ 均为主理想.

现在假设给定了无平方因子的正整数 D, 如果存在 $\mathbb{F}_p$ 上具有复乘 $R_K \subseteq \mathbb{Q}(\sqrt{-D})$ 的椭圆曲线 $\overline{E}$, 则由定理 4.13 及其推论知道 p 在 $\mathbb{Q}(\sqrt{-D})$ 中必完全分裂为两个主素理想之积, 于是 $pR_K = \pi R_K \cdot \pi' R_K$. 因 $\mathbb{Q}(\sqrt{-D})$ 中任何整元素均可表为 $\frac{x+y\sqrt{-D}}{2}$ 的形式 (x, y 为整数), 因此有

$$4p = x^2 + Dy^2. \tag{4.23}$$

可见 p 必定使得 (4.23) 式有整数解. 易知, 解 (4.23) 式等价于解 $p = u^2 + Dv^2$. 稍后将给出这个不定方程的求解方法. 一旦得到了 (4.23) 式的一个解 (x, y), 则由定理 4.13 可知 $\pi = \pi_p = \pm\frac{x+y\sqrt{-D}}{2}$, $\pi' = \pm\frac{x-y\sqrt{-D}}{2}$, 从而可知 p 次 Frobenius 映射的迹为 $\pi + \pi' = \pm x$, 可见此时 $\overline{E}(\mathbb{F}_p)$ 的元素个数为 $m = p + 1 \pm x$, 这就是 $\mathbb{F}_p$ 上具有复乘 $R_K \subset \mathbb{Q}(\sqrt{-D})$ 的椭圆曲线的可能的群阶.

现在假设有了域 $\mathbb{F}_p$ 和群阶 m, 我们要寻找 $\mathbb{F}_p$ 上的椭圆曲线 $\overline{E}$, 使得 $|\overline{E}(\mathbb{F}_p)| = m$. 此时, 下面的结果是有用的.

定理 4.14 下述各结论对 $\mathbb{F}_p$ 上的椭圆曲线成立:

(a) $\mathbb{F}_p$ 中每一个元素都是 $\mathbb{F}_p$ 上某条椭圆曲线的 j 不变量;

(b) 若 $p \geqslant 5$, 则定义在 $\mathbb{F}_p$ 上的具有给定的 j 不变量不等于 $0, 1728$ 的所有的椭圆曲线由下式给定:

$$Y^2 = X^3 + 3kc^2X + 2kc^3,$$

其中 $k = j/(1728 - j)$, c 是 $\mathbb{F}_p^*$ 中任意二次剩余.

(c) 假定 E 和 E' 具有相同的 j 不变量, 但它们不是 $\mathbb{F}_p$ 同构的, 且 $j \neq 0, 1728$, 则 E' 是 E 的 2 次扭曲, 且若 $\#E = p + 1 - t$, 则 $\#E' = p + 1 + t$.

证明 (a) 显然.

(b) 由 (4.1) 式, 可知在 $\overline{\mathbb{F}}_p$ 同构下, 具有 j 不变量 $j \neq 0, 1728$ 的椭圆曲线方程为

$$E:\ y^2 = x^3 + 3kx + 2k, \tag{4.24}$$

而任何与 E 是 $\mathbb{F}_p$ 同构的椭圆曲线由下列变换给出:

$$x = u^2X, \quad y = u^3Y, \quad u \in \mathbb{F}_p^*, \tag{4.25}$$

将其代入 (4.24) 式, 即得

$$Y^2 = X^3 + 3du^{-4}X + 2ku^{-6}.$$

令 $c = u^{-2}$, 得出

$$Y^2 = X^3 + 3kc^2X + 2kc^3, \tag{4.26}$$

反之, 直接验证, 知 (4.26) 式定义的椭圆曲线的 j 不变量为 j. 且若 c 是模 p 的二次剩余, 令 $u^2 \equiv c \pmod p$, 则由 (4.25) 式给出的同构表明 (4.24) 和 (4.26) 式是 $\mathbb{F}_p$ 同构的.

(c) 由于 E 和 E' 具有相同的 j 不变量, 故 E 和 E' 是 $\overline{\mathbb{F}}_p$ 同构的. 又由于 E 和 E' 不是 $\mathbb{F}_p$ 同构的, 且 $j(E) = j(E') \neq 0, 1728$, 故 E' 一定是 E 的某个二次扭曲 (见文献 [12] 第 X 章, 命题 5.4), 即存在一个元素 $d \in \mathbb{F}_p^* \setminus \mathbb{F}_p^{*2}$, 使得

$$\begin{aligned} E &: y^2 = x^3 + ax + b, \\ E' &: y^2 = x^3 + d^2ax + d^3b. \end{aligned} \qquad a, b \in \mathbb{F}_p.$$

对于任意 $x \in \mathbb{F}_p$, 它恰好贡献了曲线 E 上的 $\left(\frac{x^3+ax+b}{p}\right)+1$ 个有理点, 此处 $\left(\frac{\cdot}{p}\right)$ 是 Legendre 符号. 于是

$$\#E(\mathbb{F}_p) = 1 + \sum_{x\in\mathbb{F}_p}\left(\left(\frac{x^3+ax+b}{p}\right)+1\right) = 1+p+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right),$$

$$\#E'(\mathbb{F}_p) = 1 + \sum_{x\in\mathbb{F}_p}\left(\left(\frac{x^3+d^2ax+d^3b}{p}\right)+1\right) = 1+p+\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)\left(\frac{d}{p}\right),$$

此处利用了事实

$$\left(\frac{x^3+d^2ax+d^3b}{p}\right) = \left(\frac{(dy)^3+d^2a(dy)+d^3b}{p}\right) = \left(\frac{d}{p}\right)\left(\frac{y^3+ay+b}{p}\right),$$

其中 $x = dy$, 而当 x 跑遍 $\mathbb{F}_p$ 时, y 当然跑遍 $\mathbb{F}_p$. 因为 d 是模 p 的二次非剩余, 故 $\left(\frac{d}{p}\right) = -1$, 从而若 $\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right) = -t$, 则 $\sum_{x\in\mathbb{F}_p}\left(\frac{x^3+ax+b}{p}\right)\left(\frac{d}{p}\right) = t$, 证毕.

现在, 问题归结到: 哪些 j 不变量可以是 $\mathbb{F}_p$ 上一条具有给定群阶和复乘 $R_K(K = \mathbb{Q}(\sqrt{-D}))$ 的椭圆曲线 $\widetilde{E}$ 的 j 不变量?

假设这样的椭圆曲线 $\widetilde{E}$ 存在, 且它是由定理 4.12 中的约化过程所给出的, 则由前面的讨论可知, 这样的 j 不变量一定是从数域 H(H 是 K 的 Hilbert 类域) 上的对应的椭圆曲线的 j 不变量约化而来. 但后者是类多项式 $H_D(x)$ 的根, 从而 $\widetilde{j} = j(\widetilde{E})$ 是类多项式 $H_D(x)$ 在域 $\mathbb{F}_p$ 中的根. 于是我们只要求解有限域 $\mathbb{F}_p$ 上的多项式 $H_D(x)$, 则 $H_D(x)$ 在 $\mathbb{F}_p$ 上的根就是所需要的 j 不变量.

举一个例子来看上面的整个过程.

例 4.1　取 $D = 7$, 然后找一个素数 p, 使得

$$4p = x^2 + Dy^2$$

有整数解. 例如 $p = 781221660082682887337352611537$ 时, 上式有解, 于是群阶

$$m = 781221660082681210712714541668,$$

它是一个奇素数的 4 倍. $K = \mathbb{Q}(\sqrt{-7})$ 的类数 $h(K) = 1$, 于是其 Hilbert 类多项式为 1 次的. 事实上, 有 $H_7(X) = x + 3375$, 它的模 p 显然有解, 于是存在 $\mathbb{F}_p$ 上的椭圆曲线 E, 其 j 不变量为

$$j = -3375 = 781221660082682887337352608162.$$

在 $\mathbb{F}_p$ 同构意义下, 存在两条这样的曲线 (定理 4.14(c)), 它们是

$$E: Y^2 = X^3 + 3844106581359233255152052532 94X + 777088212214573747523503857 6554,$$

$$E': Y^2 = X^3 + 5863371370889685215075629773 29X + 470612877688284093511930750213.$$

现在需要确定 E 和 E' 中哪一条的阶为 m. 这可以通过随机取曲线上的点 P, 然后计算其 m 倍, 看 mP 是否为无穷远点 $\mathcal{O}$ 来解决. 最后可知 E' 是所求的曲线.

上面的计算有一个缺点, 就是一般来说 K 的 Hilbert 类多项式 $H_D(x)$ 的系数是很大的, 这给有关的计算带来不少问题. 所以, 我们希望找出 Hilbert 类域 H 的另一个生成元的极小多项式, 它们具有比 $H_D(x)$ 小得多的系数. 利用 η 函数 $\eta(\tau)$, 定义下面的 Weber 函数:

$$h(\tau) = \zeta_{48}^{-1}\frac{\eta((\tau+1)/2)}{\eta(\tau)}, \qquad h_1(\tau) = \frac{\eta(\tau/2)}{\eta(\tau)}, \quad h_2(\tau) = \sqrt{2}\frac{\eta(2\tau)}{\eta(\tau)},$$

$$\gamma_2(\tau) = \frac{h(\tau)^{24}-16}{h(\tau)^8}, \qquad \gamma_3(\tau) = \frac{(h(\tau)^{24}+8)(h_1(\tau)^8-h_2(\tau)^8)}{h(\tau)^8},$$

其中 $\zeta_n = e^{2\pi i/n}$. 不难验证

$$j = \frac{(h^{24}-16)^3}{h^{24}} = \frac{(h_1^{24}+16)^3}{h_1^{24}} = \frac{(h_2^{24}+16)^3}{h_2^{24}} = \gamma_2^3 = \gamma_3^2 + 1728.$$

称 $\mu(\tau)$ 是 $\mathbb{Q}(\tau)$ 的一个类不变量, 如果 $\mu(\tau)$ 位于 $\mathbb{Q}(\tau)$ 的 Hilbert 类域之中. 显然 $j(\tau)$ 是一个类不变量. 应用 Weber 函数, 可以决定更多的类不变量. 应用类似求 $H_D(x)$ 的方法, 可以求出这些类不变量的极小多项式 $W_D(x)$. 而从 $W_D(x)$ 模 p 的根, 可以找出所需要的 j 不变量.

Atkin 和 Morain 建议下面的各种类不变量的选择: 设 $-D$ 是一个基本判别式, d 是无平方因子的正整数, 使得 $\mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\sqrt{-d})$, 则

(1) 若 $D \equiv 3 \pmod 6$, 取 $\mu = \sqrt{-D}\gamma_3(\tau)$;

(2) 若 $D \equiv 7 \pmod 8$, 取 $\mu = h(\tau)/\sqrt{2}$;

(3) 若 $D \equiv 3 \pmod 8$, 取 $\mu = h(\tau)$;

(4) 若 $d \equiv \pm 2 \pmod 8$, 取 $\mu = h_1(\tau)/\sqrt{2}$;

(5) 若 $d \equiv 5 \pmod 8$, 取 $\mu = h(\tau)^4$;

(6) 若 $d \equiv 1 \pmod 8$, 取 $\mu = h(\tau)^2/\sqrt{2}$.

例 4.2 $D = 23 \equiv 7 \pmod 8$, 于是取 $\mu = h(\tau)/\sqrt{2}$, 可知

$$H_{23}(x) = x^3 + 3491750x^2 - 5151296875x + 23375^3,$$

$$W_{23}(x) = x^3 - x - 1.$$

§4.3 算法综述

我们在本节中讨论具体的算法实现, 它们的理论基础均在前面两节给出了详细的证明. 首先, 不难证明下述结论:

定理 4.15 设 $-D$ 是一个基本判别式, d 是无平方因子的正整数, 使得 $\mathbb{Q}(\sqrt{-D}) = \mathbb{Q}(\sqrt{-d})$, p 是一个素数, 使得方程 $p = x^2 + dy^2$ 有解, 则有

(a) 若 $p \equiv 3 \pmod 8$, 则 $D \equiv 2, 3$或$7 \pmod 8$;

(b) 若 $p \equiv 5 \pmod 8$, 则 $D \equiv 1 \pmod 2$;

(c) 若 $p \equiv 7 \pmod 8$, 则 $D \equiv 3, 6$或$7 \pmod 8$.

特别地, 我们有 $\left(\frac{-d}{p}\right) = \left(\frac{-D}{p}\right) = 1$.

首先, 考虑类群和类数的计算, 由定理 4.4, 任何一个二元二次型仅与一个既约形式相似, 于是只要找出所有的既约形式即可.

(算法 4.1) Class_Group 算法

输入: 一个无平方因子的正整数 D.

输出: 类群 $CL(D)$.

Step 1: 令 $S = \lfloor\sqrt{D/3}\rfloor$;

Step 2: 对于 B 从 0 到 S, 计算

2.1 列出 $D + B^2$ 的所有正因子 $A_1, A_2, \cdots, A_r$, 满足 $2B \leqslant A_i \leqslant \sqrt{D + B^2}$;

2.2 对于 i 从 1 到 r, 计算

2.2.1 置 $C = (D + B^2)/A_i$;

2.2.2 若 $\gcd(A_i, 2B, C) = 1$, 则列出 $\{A_i, B, C\}$, 若 $0 < 2B < A_i < C$, 则列出 $\{A_i, -B, C\}$.

Step 3: 输出列表.

其次, 考虑类多项式. 令

$$\begin{aligned} F(z) &= 1 + \sum_{j=1}^{\infty}(-1)^j\left(z^{(3j^2-j)/2} + z^{(3j^2+j)/2}\right) \\ &= 1 - z - z^2 + z^5 + z^7 - z^{12} - z^{15} + \cdots \\ \theta &= \exp\left(\frac{-\sqrt{D} + Bi}{A}\pi\right), \end{aligned}$$

置

$$f_0(A,B,C)=\theta^{-1/24}F(-\theta)/F(\theta^2),$$
$$f_1(A,B,C)=\theta^{-1/24}F(\theta)/F(\theta^2),$$
$$f_2(A,B,C)=\sqrt{2}\theta^{1/12}F(\theta^4)/F(\theta^2).$$

若 $\{A,B,C\}$ 是正定二元二次型, $D=AC-B^2$, 则定义其类不变量为

$$[A,B,C]=\left(N\lambda^{-BL}2^{-I/6}(f_J(A,B,C)^K)\right)^G,$$

其中

$$G=\gcd(D,3),\quad \lambda=e^{\pi iK/24},$$

$$I=\begin{cases}3, & 若\ D\equiv 1,2,6,7 \pmod 8,\\ 0, & 若\ D\equiv 3 \pmod 8 且\ D\not\equiv 0 \pmod 3,\\ 2, & 若\ D\equiv 3 \pmod 8 且\ D\equiv 0 \pmod 3,\\ 6, & 若\ D\equiv 5 \pmod 8;\end{cases}$$

$$J=\begin{cases}0, & 若\ AC\ 奇,\\ 1, & 若\ C\ 偶,\\ 2, & 若\ A\ 偶;\end{cases}\qquad K=\begin{cases}2, & 若\ D\equiv 1,2,6 \pmod 8,\\ 1, & 若\ D\equiv 3,7 \pmod 8,\\ 4, & 若\ D\equiv 5 \pmod 8;\end{cases}$$

$$L=\begin{cases}A-C+A^2C, & 若\ AC\ 奇或\ D\equiv 5 \pmod 8\ 且\ C\ 偶,\\ A+2C-AC^2, & 若\ D\equiv 1,2,3,6,7 \pmod 8\ 且\ C\ 偶,\\ A-C+5AC^2, & 若\ D\equiv 3 \pmod 8\ 且\ A\ 偶,\\ A-C-AC^2, & 若\ D\equiv 1,2,5,6,7 \pmod 8\ 且\ A\ 偶;\end{cases}$$

$$M=\begin{cases}(-1)^{(A^2-1)/8}, & 若\ A\ 奇,\\ (-1)^{(C^2-1)/8}, & 若\ A\ 偶;\end{cases}$$

$$N=\begin{cases}1, & 若\ D\equiv 5 \pmod 8\ 或\ D\equiv 3 \pmod 8,\ AC\ 奇或\ D\equiv 7 \pmod 8,\ AC\ 偶,\\ M, & 若\ D\equiv 1,2,6 \pmod 8\ 或\ D\equiv 7 \pmod 8\ 且\ AC\ 奇,\\ -M, & 若\ D\equiv 3 \pmod 8\ 且\ AC\ 偶.\end{cases}$$

若 $\{A_1,B_1,C_1\},\cdots,\{A_h,B_h,C_h\}$ 是判别式为 $-D$(D 为无平方因子正整数) 的全体既约正定二次型, 则定义对应于 D 的约化类多项式为

$$W_D(t)=\prod_{j=1}^{h}\left(t-[A_j,B_j,C_j]\right).$$

约化的类多项式具有整系数.

第 3 步, 我们考虑复乘.

(算法 4.2) CM_Discriminant 算法

输入: 一个素数 p, 一个无平方因子的正整数 D, D 满足定理 4.15 中的同余式.

输出: 如果方程 $4p = W^2 + DV^2$ 有解, 则输出 W, 若无解, 则输出 "D 不是一个复乘判别式".

Step 1: 求出 $-D$ 模 p 的平方根, 或决定这样的平方根不存在;

Step 2: 若 Step 1 的结果是平方根不存在, 则输出 "D 不是一个复乘判别式"; 否则, 令 B 是 $-D$ 模 p 的一个平方根.

Step 3: 置 $A = p, C = (B^2 + D)/p$;

Step 4: 令 $S = \begin{pmatrix} A & B \\ B & C \end{pmatrix}$, $U = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$;

Step 5: 除非 $|2B| \leqslant A \leqslant C$, 重复下列步骤:

　5.1 令 $\delta = \lfloor \frac{B}{C} + \frac{1}{2} \rfloor$;

　5.2 令 $T = \begin{pmatrix} 0 & -1 \\ 1 & \delta \end{pmatrix}$;

　5.3 用 $T^{-1}U$ 代替 U;

　5.4 用 T^tST 代替 S, (T^t 表示 T 的转置)

Step 6: 若 $D = 11$ 且 $A = 3$, 令 $\delta = 1$, 并重复 5.2, 5.3, 5.4;

Step 7: 令 X 和 Y 是 U 的元素, 即 $U = \begin{pmatrix} X \\ Y \end{pmatrix}$;

Step 8: 若 $D = 1$ 或 3, 输出 $W = 2X$ 且 $V = 2Y$, 程序终止;

Step 9: 若 $A = 1$, 输出 $W = 2X$, 程序终止;

Step 10: 若 $A = 4$, 输出 $W = 4X + BY$, 程序终止;

Step 11: 输出 "D 不是一个复乘判别式".

第 4 步, 我们考虑可能的椭圆曲线的群阶.

(算法 4.3) EC_Order 算法

输入: 一个素数 p.

输出: 一个无平方因子的正整数 D 及一个正整数 u, 使得 u 是 $\mathbb{F}_p$ 上某条具有复乘 $R_K(K=\mathbb{Q}(\sqrt{-D}))$ 的椭圆曲线的阶.

Step 1: 选取一个无平方因子正整数 D, D 满足定理 4.15 中的同余式;

Step 2: 计算 Jacobi 符号 $J=\left(\frac{-D}{p}\right)$, 若 $J=-1$, 返回 Step 1;

Step 3: 列出 D 的所有奇素因子 l;

Step 4: 对每个 l, 计算 Jacobi 符号 $J=\left(\frac{p}{l}\right)$, 若对某个 l 有 $J=-1$, 则返回 Step 1;

Step 5: 利用 CM_Discuriminant, 决定 D 是否为一个对于 p 的复乘判别式, 若不是, 则返回 Step 1, 否则, 有整数 W(若 $D=1$ 或 3, 还有整数 V);

Step 6: 列出所有可能的阶如下:

- 若 $D=1$, 阶为 $u=p+1\pm W$ 或 $p+1\pm V$;
- 若 $D=3$, 阶为 $u=p+1\pm W$ 或 $p+1\pm(W+3V)/2$ 或 $p+1\pm(W-3V)/2$;
- 否则, 阶为 $u=p+1\pm W$.

Step 7: 输出 (D,u), 程序结束.

第 5 步, 构造具有给定复乘的椭圆曲线.

(算法 4.4) Curve_Prescribed_CM 算法

输入: 一个素数 p 及对于 p 的一个复乘判别式 D.

输出: $a_0, b_0 \in \mathbb{F}_p$, 使得椭圆曲线

$$E_0:\ y^2=x^3+ax+b(\mathrm{mod}\ p)$$

具有复乘 $R_K(K=\mathbb{Q}(\sqrt{-D}))$.

Step 1: 若 D 是下列 9 个值, 则直接写出相应的 a_0 和 b_0 如下:

D	a_0	b_0
1	1	0
2	-30	56
3	0	1
7	-35	98
11	-264	1694
19	-152	722
43	-3440	77658
67	-29480	1948226
163	-8697680	9873093538

Step 2：计算约化的类多项式 $W(t) = W_D(t)$;

Step 3：W =CM_Discriminant(p, D);

Step 4：若 W 是偶数, 找出 $W(t)\text{mod } p$ 的一个线性因子 $t - s$, 令

$$V := (-1)^D 2^{4I/K} S^{24/(GK)} (\text{mod } p),$$

$$a_0 := -3(V + 64)(V + 16)(\text{mod } p),$$

$$b_0 := 2(V + 64)^2(V - 8)(\text{mod } p);$$

Step 5：若 W 是奇数, 找出 $W(t)\text{mod } p$ 的一个立方因子 $g(t)$, 计算

$$V(t) := \begin{cases} -t^{24}(\text{mod } g(t)), & \text{若} 3 \nmid D, \\ -256t^8(\text{mod } g(t)), & \text{若} 3 | D, \end{cases}$$

$$a_1(t) := -3\big(V(t) + 64\big)\big(V(t) + 256\big)(\text{mod } g(t)),$$

$$b_1(t) := 2\big(V(t) + 64\big)^2\big(V(t) - 512\big)(\text{mod } g(t)),$$

$$a_3(t) := a_1(t)^3(\text{mod } g(t)),$$

$$b_2(t) := b_1(t)^2(\text{mod } g(t)),$$

现在设 σ 是 $a_3(t)$ 的一个非零系数, 而 τ 是 $b_2(t)$ 的对应的系数, 令

$$a_0 := \sigma\tau(\text{mod } p), \qquad b_0 := \sigma\tau^2(\text{mod } p);$$

Step 6：输出 (a_0, b_0), 程序结束.

第 6 步, 找出所需要的椭圆曲线

(算法 4.5) Find_Curve 算法

输入：椭圆曲线参数 p, u, 以及由 (a_0, b_0)=Curve_Prescribed_CM(p, D).

输出：一条椭圆曲线 $E/\mathbb{F}_p$, 使得 $\#E(\mathbb{F}_p) = u$.

Step 1：选取整数 ξ, $0 < \xi < p$,

Step 2：若 $D = 1$, 则令 $a = a_0\xi \pmod p$, $b = 0$; 若 $D = 3$, 则令 $a = 0$ 且 $b = b_0\xi \pmod p$; 否则, 令 $a = a_0\xi^2 \pmod p$, $b = b_0\xi^3 \pmod p$;

Step 3：随机选取 $y^2 = x^3 + ax + b$ 上的一些点 P, 计算 uP, 若 $uP \neq \mathcal{O}$, 则返回 Step 1;

Step 4：若对随机选取的若干点 P, 均有 $uP = \mathcal{O}$, 则输出

$$E: \ y^2 = x^3 + ax + b.$$

在算法 Curve-Prescribed-CM 中, 需要计算一个多项式的不可约因子, 这可由下述算法给出：

(算法 4.6) Irreducible_Factor 算法

输入：素数 $p > 2$, 正整数 d, 多项式 $f(t)$, $f(t) \bmod p$ 分解为次数 d 的不同的不可约因子之积.

输出：$f(t)$ 的一个次数为 d 的因子 $g(t)$.

Step 1：令 $g(t) = f(t)$;

Step 2：若 $\deg(g) > d$

2.1 随机选取一个次数 $2d-1$ 的首一多项式 $u(t)$,

2.2 计算 $c(t) := u(t)^{(p^d-1)/2} \pmod{g(t)}$,

2.3 令 $h(t) = \gcd\left(c(t)-1, g(t)\right)$,

2.4 若 $h(t)$ 为常数或 $\deg(h) = \deg(g)$, 返回 Step 2.1,

2.5 若 $2\deg(h) > \deg(g)$, 令 $g(t) = g(t)/h(t)$; 否则, 令 $g(t) = h(t)$;

Step 3：输出 $g(t)$.

第五章　椭圆曲线的 SEA 算法

§5.1　算法的概述

设 p 为奇素数, E 为定义在 $\mathbb{F}_p$ 上的椭圆曲线,

$$E: \quad y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \neq 0,\ a, b \in \mathbb{F}_p, \tag{5.1}$$

记

$$E(\mathbb{F}_p) = \{(u, v) | v^2 = u^3 + au + b,\ u, v \in \mathbb{F}_p\} \bigcup \{\mathcal{O}\},$$

则有 ((3.21) 式)

$$\#E(\mathbb{F}_p) = p + 1 - t,$$

其中 t 为 E 上的 p 阶 Frobenius 映射

$$\begin{aligned} \phi: \quad E &\longrightarrow E \\ (x, y) &\longmapsto (x^p, y^p) \\ \mathcal{O} &\longmapsto \mathcal{O} \end{aligned}$$

的迹, 且 $|t| \leqslant 2\sqrt{p}$(定理 3.18).

Schoof-Elkies-Arkin 算法 (SEA 算法) 是计算 $\#E(\mathbb{F}_p)$ 的有效算法. 计算 $\#E(\mathbb{F}_p)$ 归结为计算 t, 若对足够多的奇素数 $l\,(\neq p)$, 算出 $t \bmod l$, 当这些 l 的乘积

$$\prod_{l \geqslant 3} > 4\sqrt{p}$$

时, 就可由中国剩余定理得到 t.

将 E 看作 $\overline{\mathbb{F}}_p$ 上的椭圆曲线, 由于 $l \neq p$, E 上的 l 阶点集合为

$$E[l] \simeq \mathbb{Z}/l\mathbb{Z} \otimes \mathbb{Z}/l\mathbb{Z},$$

(定理 3.14), 因此可以看作 $\mathbb{F}_l$ 上的 2 维向量空间, 由于 $[l] \cdot \phi = \phi \cdot [l]$, 所以

$$\phi\big(E[l]\big) \subset E[l],$$

ϕ 生成 $E[l]$ 上的一个线性变换, 将它记为 ϕ_l(它实际上是 §3.5 中定义的 ϕ_l 在 $E[l]$ 上的限制). ϕ_l 的特征多项式为

$$\overline{f}(x) = x^2 - tx + p \pmod{l}, \tag{5.2}$$

ϕ_l 的迹为 $t \bmod l$.

为了计算 $t \bmod l$, Schoof [16] 提出下述算法: 记 $t' \equiv t(\bmod\ l)$, $p' \equiv p(\bmod\ l)$, 则对所有的 $(x, y) \in E[l]$, 有

$$\phi^2(x, y) + p'(x, y) = t'\phi(x, y).$$

即

$$(x^{p^2}, y^{p^2}) + p'(x, y) \equiv t'(x^p, y^p)(\bmod\ y^2 - x^3 - ax - b,\ f_l(x)),$$

这里 $f_l(x)$ 是 §2.4 中定义的除子多项式 (见推论 2.3), 它的次数为 $(l^2 - 1)/2$.

考虑 Schoof 算法的计算量, 设 $\prod_{l \leqslant l_{\max}} > 4\sqrt{p}$, 即 $\sum_{l \leqslant l_{\max}} \log l > \log\left(4\sqrt{p}\right)$. 由素数定理 ($\sum_{p<x} \log p \sim x$), 可知 $l_{\max} = O\big(\log p\big)$, 而

$$\#\{l \,|\, l \leqslant l_{\max}\} = O\big(\log p / \log\log p\big),$$

所以需要计算的素数 l 的个数为 $O(\log p)$. 上述计算都是在环

$$\mathbb{F}_p[x, y]/(f_l(x), y^2 - x^3 - ax - b)$$

中进行的, 该环的元素个数为 $l^2 \log p$, 我们需要在该环中计算 x^p, x^{p^2}, y^p, y^{p^2} 等, 每次乘法需要计算量为 $(l^2 \log p)^2$, 这部分的计算量为 $O\big(\log p(l^2 \log p)^2\big)$. (x^p, y^p) 需进行 t' 次加法, 而 t' 从 1 跑至 l, 这部分计算量为 $O\big(l(l^2 \log p)^2\big)$. 对每个 l 都需进行上述计算, 而 l 的个数为 $O\big(\log p\big)$, 所以 Schoof 算法的计算量为 $O\big(\log^8 p\big)$, 这是一个多项式时间的算法, 从渐近意义上讲应该算得很快, 但实际上这个算法并不实用, 主要问题是 $f_l(x)$ 的次数太高 (l^2 阶). 例如, 当 $l > 250$ 时, 存储 $\mathbb{F}_p[x, y]/(\phi_l, y^2 - x^3 - ax - b)$ 中一个元素就需上百万个字节.

Atkin 和 Elkies 改进了 Schoof 算法, 使其成为一个实际可行的算法, 其中一个重要的改进是利用除子多项式 $f_l(x)$ 的一个次数为 $(l-1)/2$ 的因子代替 $f_l(x)$, 现在利用 SEA 算法, 在一般的 PC 机上, 大约半分钟可以计算一条 192 比特的椭圆曲线的点数.

若能找到 (5.2) 式的一个根 α(即为 ϕ_l 的本征根), 则另一个根为 p/α, 这时 $t = \alpha + p/\alpha$, 当 (5.2) 式在 $\mathbb{F}_l$ 中有根时, l 称为 Elkies 素数, 否则 l 称为 Atkin 素数. 当 l 为 Elkies 素数时, $t \bmod l$ 可以惟一确定, 而当 l 为 Atkin 素数时, 仅能得到几个可能的 $t \bmod l$(见 §5.5).

当 l 为 Elkies 素数时, 在 $E[l]$ 中存在 ϕ_l 的本征子空间, 它是 1 维向量空间. 在 Elkies 算法中, 先确定 ϕ_l 的本征子空间, 然后再计算其对应的本征根 α. $E[l]$ 中共有 $l+1$ 个 1 维子空间, 若以 e_1 和 e_2 表示 $E[l]$ 的一组基, 则 $l+1$ 个子空间为

$$\mathcal{C}_0 = \{ke_1 \mid k = 0, 1, \cdots, l-1\},$$
$$\mathcal{C}_i = \{k(ie_1 + e_2) \mid k = 0, 1, \cdots, l-1\}, \quad i = 1, 2, \cdots, l,$$

每个 $\mathcal{C}_i$ 也可看作 E 的 l 阶循环子群. 由于 a 和 b 都可看作整数, 所以 E 可看作复数域 $\mathbb{C}$ 上的椭圆曲线, 因而第一章的很多结果可应用于 E. 由命题 2.4, 对每个 $\mathcal{C}_i$, 存在 E 的一个同种曲线 $E_i \simeq E/\mathcal{C}_i$, 而 $j(E_i)$ 是 l 阶模多项式 $\Phi_l(x, j(E)) \pmod p$(因 $\Phi_l(x, j(E)$ 的系数都是整数, 将系数模 p 后可看作 $\mathbb{F}_p$ 上的多项式) 的根 (定理 2.10), 其中

$$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2} \pmod p$$

(见 (2.6) 式). 推论 2.2 同样给出了 $\mathbb{F}_p$ 上的同种映射 $E \to E/\mathcal{C}_i$ 的表达式. $\Phi_l(x, j(E))$ 是 $\mathbb{F}_p$ 上 x 的 $l+1$ 次多项式, 它在 $\overline{\mathbb{F}_p}$ 中的 $l+1$ 个根即为 $j(E_i)\,(0 \leqslant i \leqslant l)$. 当 $j(E_i)$ 确定后, E_i 在同构意义下就惟一确定, 例如当 $j(E_i) \neq 0, 1728$ 时, 取

$$a_i = b_i = \frac{27j(E_i)}{4(1728 - j(E_i))},$$

E_i 即为

$$y^2 = x^3 + a_i x + b_i,$$

所以当 $j(E_i) \in \mathbb{F}_{p^r}$ 时, E_i 是定义在 $\mathbb{F}_{p^r}$ 上的椭圆曲线 (当 $j(E_i) = 0$ 或 1728 时, 结论也同样成立). 可以证明, l 为 Elkies 素数时, 当且仅当 $\Phi_l(x, j(E))$ 在 $\mathbb{F}_p$ 中有根 (推论 5.1), 因而要判断 l 是否是 Elkies 素数, 仅需判断

$$\gcd\left(x^p - x, \Phi_l(x, j(E))\right) \tag{5.3}$$

的次数是否 $\geqslant 1$.

当 l 为 Elkies 素数时, 利用 (5.3) 式计算 $\Phi_l(x, j(E))$ 在 $\mathbb{F}_p$ 中的根, 就可以得到 E 的一条同种曲线 (见 §5.3)

$$\widehat{E}: \quad y^2 = x^3 + \widehat{a}x + \widehat{b}, \quad \widehat{a}, \widehat{b} \in \mathbb{F}_p.$$

由 E 到 $\widehat{E}$ 的同种映射的核为某个 $\mathcal{C}_i$, 记为 $\mathcal{C}^* = \mathbb{F}_l \cdot e$, 我们有 $\phi(\mathcal{C}^*) = \mathcal{C}^*$(定理 5.1), 从而存在 $\alpha \in \mathbb{F}_l$, 使得 $\phi(e) = \alpha e$, 即 α 为 ϕ 的本征值, 于是

$$t = \alpha + p/\alpha (\text{mod } l).$$

在 Elikes 算法中, 实际上并不能直接给出本征子空间 C^*, 而是计算

$$h(x)=\prod_{\theta\in C^*/\{\pm1\}}(x-x(\theta)),$$

这里 $x(\theta)$ 为 θ 点的 x 坐标, $h(x)$ 为 $d=(l-1)/2$ 次多项式. $h(x)$ 是 C^* 中点的 x 坐标所适合的方程, 它是推论 2.3 中除子多项式 $f_l(x)$ 的因子. 由于 $\phi\big(h(x)\big)=h(x)$, $h(x)$ 是 $\mathbb{F}_p$ 上的多项式.

得到 $h(x)$ 后, 在 $\mathbb{F}_l$ 中寻找 α, 使得

$$(x^p,y^p)\equiv\alpha(x,y)\pmod{y^2-x^3-ax-b,h(x)},$$

即可找到 ϕ_l 的本征根. 由于 $h(x)$ 的次数为 $(l-1)/2$, 而 $f_l(x)$ 的次数为 $(l^2-1)/2$, 所以 Elkies 算法改进了 Schoof 算法.

本章的 §5.2~§5.4 介绍 Elkies 算法, §5.5 介绍 Atkin 算法.

§5.2 等价模多项式

在 §2.5 中定义的模多项式 $\Phi_l(x,y)\in\mathbb{Z}[x,y]$ 的系数当 l 增大时, 会非常迅速地增大, 这增加了使用 Φ_l 时计算的复杂性, 以 $l=3$ 为例,

$$\begin{aligned}\Phi_3(x,y)=&x^4-x^3y^3+y^4+2232(x^3y^2+y^3x^2)-1069956(x^3y+y^3x)\\&+36864000(x^3+y^3)+2587918086x^2y^2+8900222976000(x^2y+y^2x)\\&+452984832000000(x^2+y^2)-770845966336000000xy\\&+1855425871872000000000(x+y),\end{aligned}$$

以 $h(\Phi_l)$(l 为素数) 表示 $\Phi_l(x,y)$ 的系数的最大绝对值的自然对数, 则可以证明

$$h(\Phi_l)=6(l+1)\Big(\Big(1-\frac{2}{l}\Big)\log l+O(1)\Big).$$

我们将利用一个等价的模多项式 $\Phi_l^c(x,y)\in\mathbb{Z}[x,y]$, 它仍是 x 的 $l+1$ 次多项式, 具有 $\Phi_l(x,y)$ 的很多性质, 但它的系数要小很多.

取 s 为最小正整数, 使得 $v=s(l-1)/12$ 为整数, 定义

$$g(\tau)=l^s\Big(\frac{\eta(l\tau)}{\eta(\tau)}\Big)^{2s},\qquad\tau\in\mathfrak{H},\tag{5.4}$$

其中

$$\begin{aligned}\eta(\tau)&=q^{1/24}\prod_{n\geqslant1}(1-q^n)\\&=q^{1/24}\Big(1+\sum_{n=1}^{\infty}(-1)^n\big(q^{n(3n-1)/2}+q^{n(3n+1)/2}\big)\Big),\end{aligned}\qquad q=e^{2\pi i\tau}.$$

引理 5.1　设 a,b,c,d 为整数, $ad-bc=1$, 则

$$\eta\Big(\frac{a\tau+b}{c\tau+d}\Big)=\varepsilon\cdot\sqrt{c\tau+d}\cdot\eta(\tau),$$

其中 ε 为 24 次单位根, 由下式确定:

当 d 为正奇数时: $\varepsilon=\left(\frac{c}{d}\right)i^{(d-1)/2}\cdot\exp\left(\frac{\pi i}{12}[d(b-c)-(d^2-1)ac]\right)$,

当 c 为正奇数时: $\varepsilon=\left(\frac{c}{d}\right)i^{(1-c)/2}\cdot\exp\left(\frac{\pi i}{12}[c(a+d)-(c^2-1)bd-3]\right)$,

($\left(\frac{d}{c}\right)$ 为 Jacobi 符号), 特别有

$$\eta\Big(\frac{1}{\tau}\Big)=\sqrt{-i\tau}\eta(\tau).$$

证明见文献 [13].

令

$$\Gamma_0(l)=\left\{\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in SL_2(\mathbb{Z})\,\middle|\, l|c\right\}.$$

命题 5.1　设 $\alpha=\begin{pmatrix} a & b\\ c & d\end{pmatrix}\in\Gamma_0(l)$, 则

$$g\circ\alpha=g\Big(\frac{a\tau+b}{c\tau+d}\Big)=g(\tau).$$

证明　由引理 5.1, 有

$$g\Big(\frac{a\tau+b}{c\tau+d}\Big)=l^s\left(\frac{\eta\left(\frac{a\cdot l\tau+lb}{l\tau\cdot c/l+d}\right)}{\eta\left(\frac{a\tau+b}{c\tau+d}\right)}\right)^{2s}=l^s\left(\frac{\varepsilon_1\sqrt{c\tau+d}\eta(l\tau)}{\varepsilon_2\sqrt{c\tau+d}\eta(\tau)}\right)^{2s},$$

故仅需证明 $(\varepsilon_1/\varepsilon_2)^{2s}=1$, 设 d 为正奇数 (若 c 为正奇数可类似地证明),

$$\begin{aligned}\Big(\frac{\varepsilon_1}{\varepsilon_2}\Big)^{2s}&=\left(\frac{\left(\frac{c/l}{d}\right)i^{(d-1)/2}\cdot\exp\left(\frac{\pi i}{12}[d(bl-c/l)-(d^2-1)ac/l]\right)}{\left(\frac{c}{d}\right)i^{(d-1)/2}\cdot\exp\left(\frac{\pi i}{12}[d(b-c)-(d^2-1)ac]\right)}\right)^{2s}\\&=\exp\left(\frac{s(l-1)}{12}\cdot 2\pi i[d(b+c/l)+(d^2-1)ac/l]\right)=1.\end{aligned}$$

证毕.

令

$$W_l=\begin{pmatrix} 0 & -1\\ l & 0\end{pmatrix},$$

则

$$g\circ W_l=g(-1/l\tau)=l^s\left(\frac{\eta(-1/\tau)}{\eta(-1/l\tau)}\right)^{2s}=l^s\left(\frac{\sqrt{-i\tau}\eta(\tau)}{\sqrt{-il\tau}\eta(l\tau)}\right)^{2s}=\left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s}. \quad (5.5)$$

记

$$f(\tau)=\left(\frac{\eta(\tau)}{\eta(l\tau)}\right)^{2s}=l^s/g(\tau),$$

由于

$$W_l\cdot\Gamma_0(l)\cdot W_l^{-1}=\Gamma_0(l),$$

故对任一 $\alpha\in\Gamma_0(l)$, 有 $f\circ\alpha=f$.

引理 5.2 *模群 $SL_2(\mathbb{Z})$ 关于其子群 $\Gamma_0(l)$ 有陪集分解*

$$SL_2(\mathbb{Z})=\Gamma_0(l)\bigcup_{k=0}^{l-1}\Gamma_0(l)\begin{pmatrix}0&-1\\1&k\end{pmatrix}.$$

证明 任取 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in SL_2(\mathbb{Z})$, 若 $l|c$, 则 $\left(\begin{smallmatrix}a&b\\c&d\end{smallmatrix}\right)\in\Gamma_0(l)$, 设 $l\nmid c$, 这时 $(c,la)=1$, 存在 $u,v\in\mathbb{Z}$, 使得 $lau+cv=1$, 从而

$$\begin{pmatrix}c&-a\\lu&v\end{pmatrix}\begin{pmatrix}a&b\\c&d\end{pmatrix}=\begin{pmatrix}0&-1\\1&blu+vd\end{pmatrix}.$$

又由于

$$\begin{pmatrix}1&0\\lc&1\end{pmatrix}\begin{pmatrix}0&-1\\1&k\end{pmatrix}=\begin{pmatrix}0&-1\\1&k-lc\end{pmatrix},$$

证毕.

$g(\tau)$ 有关于 $q=e^{2\pi i\tau}$ 的展开式:

$$g(\tau)=l^s\left(\frac{q^{l/24}\prod(1-q^{ln})}{q^{1/24}\prod(1-q^n)}\right)^{2s}=l^sq^v\left(\frac{\prod(1-q^{ln})}{\prod(1-q^n)}\right)^{2s}=l^sq^v+\sum_{n=v+1}^{\infty}a_nq^n, \quad (5.6)$$

其中 a_n 为整数. 同样, $f(\tau)$ 有 q 展开式

$$f(\tau)=q^{-v}\left(\frac{\prod(1-q^n)}{\prod(1-q^{ln})}\right)^{2s}=q^{-v}+\sum_{n=-v+1}^{\infty}b_nq^n. \quad (5.7)$$

定义 $l+1$ 次多项式

$$k(X)=(x-g(\tau))\prod_{k=0}^{l-1}\left(x-g\left(\frac{-1}{\tau+k}\right)\right). \quad (5.8)$$

$k(X)$ 的系数是 $g(\tau)$, $g\left(\frac{-1}{\tau+k}\right) = g \circ \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ $(0 \leqslant k \leqslant l-1)$ 的初等对称多项式, 由命题 5.1 和引理 5.2, 对任一 $\alpha \in SL_2(\mathbb{Z})$, $g \circ \alpha$, $g \circ \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix} \cdot \alpha$ $(0 \leqslant k \leqslant l-1)$ 是 g, $g \circ \begin{pmatrix} 0 & -1 \\ 1 & k \end{pmatrix}$ $(0 \leqslant k \leqslant l-1)$ 的一个置换, 故 $k(X)$ 的系数在 α 作用下不变, 又由于 (5.6) 和 (5.7) 式 (注意: $g\left(\frac{-1}{\tau+k}\right) = f\left(\frac{\tau+k}{l}\right)$), $k(X)$ 的系数都有 q 展开式, 仅具有有限个 q 的负幂次项, 所以 $k(X)$ 的系数都是模群上的模函数, 它们可以表成 $j(\tau)$ 的整数系数多项式 (引理 2.2), 即 $k(X) \in \mathbb{Z}[X, j(\tau)]$. 记

$$\Phi_l^c\big(x, j(\tau)\big) = k(x) = \sum_{r=0}^{l+1} \left(\sum_{k=0}^{v} a_{r,k} j(\tau)^k \right) x^r, \qquad a_{r,k} \in \mathbb{Z}. \tag{5.9}$$

在 (5.9) 式中, 以 $l\tau$ 代替 τ, 由于

$$g(l\tau) = l^s / f(l\tau),$$

$$g\left(\frac{-1}{\tau+k}\right) = g\left(\frac{-1}{l(\tau+k/l)}\right) = f(\tau + k/l), \quad 0 \leqslant k \leqslant l-1,$$

(5.9) 式变为

$$\Phi_l^c\big(x, j(l\tau)\big) = \big(X - l^s/f(l\tau)\big) \prod_{k=0}^{l-1} \left(X - f\left(\tau + \frac{k}{l}\right) \right), \tag{5.10}$$

可见 $\Phi_l^c\big(f(\tau), j(l\tau)\big) = 0$, 即

$$\sum_{r=0}^{l+1} \left(\sum_{k=0}^{v} a_{r,k} j(l\tau)^k \right) f(\tau)^r = 0.$$

利用上式可计算系数 $\{a_{r,k} \,|\, 0 \leqslant r \leqslant l+1,\ 0 \leqslant k \leqslant v\}$.

令

$$s_r(\tau) = \sum_{k=0}^{v} a_{l+1-r,k} \cdot j(l\tau)^k,$$

$$c_r(\tau) = \sum_{k=0}^{l-1} f\left(\tau + \frac{k}{l}\right)^r + \left(\frac{l^s}{f(l\tau)}\right)^r = c_{r,1}(\tau) + c_{r,2}(\tau),$$

利用牛顿公式得到

$$s_r(\tau) = \frac{(-1)^r}{r} \sum_{m=1}^{r} (-1)^{m-1} c_m(\tau) s_{r-m}(\tau). \tag{5.11}$$

设

$$f(\tau)^r = q^{-vr}\sum_{m=0}^{\infty} a_m q^m,$$

则

$$\begin{aligned}
c_{r,1}(\tau) &= \sum_{k=0}^{l-1} f\left(\tau+\frac{k}{l}\right)^r \\
&= \sum_{k=0}^{l-1} e^{-2\pi i(\tau+k/l)vr}\sum_{m=0}^{\infty} a_m e^{2\pi i(\tau+k/l)m} \\
&= q^{-vr}\sum_{m=0}^{\infty} a_m q^m \sum_{k=0}^{l-1} e^{2\pi i k(m-vr)/l} \\
&= l\sum_{d\geqslant -\lfloor \frac{vr}{l}\rfloor} a_{ld+vr} q^{ld}.
\end{aligned} \tag{5.12}$$

利用上述算法可以计算模多项式 $\Phi_l^c(x,y)$(见算法 5.1). 下面是 $l=3,5,7$ 的例子:

$$\begin{aligned}
\Phi_3^c(x,y) &= x^4+36x^3+270x^2-(y-756)x+729, \\
\Phi_5^c(x,y) &= x^6+30x^5+315x^4+1300x^3+1575x^2-(y-750)x+125, \\
\Phi_7^c(x,y) &= x^8+28x^7+322x^6+1904x^5+5915x^4+8624x^3+4018x^2 \\
&\quad -(y-748)x+49.
\end{aligned}$$

多项式 $\Phi_l^c(x,y)$ 与 §2.5 中所定义的模多项式 $\Phi_l(x,y)$ 有很多类似的性质 (见定理 5.2 和文献 [17]), 但它的系数要小得多, 便于应用.

定理 5.1 设 E 不是超奇异且 $j(E)\neq 0,1728$, ϕ 为 E 上 p 阶 Frobenius 映射, $\mathcal{C}_i\,(0\leqslant i\leqslant l)$ 为 $E[l]$ 中的 $l+1$ 个 l 阶子群, 设 d_i 为最小正整数, 使得 $\phi^{d_i}(\mathcal{C}_i)=\mathcal{C}_i$, 则 $j\big(E/\mathcal{C}_i\big)\in\mathbb{F}_{p^{d_i}}$, 且 d_i 也是使该式成立的最小正整数.

证明 若 $\phi^{d_i}(\mathcal{C}_i)=\mathcal{C}_i$, 这时推论 2.2 中的同种映射 $\varphi: E\to E/\mathcal{C}_i$ 定义在域 $\mathbb{F}_{p^{d_i}}$ 上, 由此可推得 $j\big(E/\mathcal{C}_i\big)\in\mathbb{F}_{p^{d_i}}$. 关于这个定理的详细证明, 参阅文献 [18] 的命题 1.6 (当 $E[p]=\{\mathcal{O}\}$ 时, E 称为超奇异, 这时 $\#E(\mathbb{F}_p)=p+1$).

注: 当 $j(E)=0$ 或 1728 时, 存在更简单的方法计算 $\#E(\mathbb{F}_p)$. E 为超奇异曲线的概率是非常小的, 所以定理 5.1 的假设条件在实用上不重要.

由定理 5.1 可知, $E/\mathcal{C}_i$ 的定义域由 $\Phi_l\big(x,j(E)\big) \pmod p$ 在 $\mathbb{F}_p$ 上的不可约因子的次数所决定. 若存在某 $\mathcal{C}_i$, 使得 $\phi(\mathcal{C}_i)=\mathcal{C}_i$ 时, l 就是 Elkies 素数, 所以有

推论 5.1 当且仅当 $\Phi_l\big(x,j(E)\big) \pmod p$ 在 $\mathbb{F}_p$ 中有根时, l 为 Elkies 素数.

定理 5.2　设 $g(\tau)$ 为 $\Gamma_0(l)$ 上的模函数, 则

$$G_l(x,j(\tau))=(x-g(\tau))\prod_{k=0}^{l-1}\left(x-g\left(\frac{-1}{\tau+k}\right)\right)$$

属于 $\mathbb{Z}[x,j(\tau)]$, 且 $G_l\big(x,j(E)\big) \pmod p$ 与 $\Phi_l\big(x,j(E)\big) \pmod p$ 在 $\mathbb{F}_p$ 上有相同的因子分解模式 (具有相同的不可约因子次数的集合).

证明见文献 [19] 的推论 4.33.

可见 $\Phi_l^c\big(x,j(E)\big)$ 与 $\Phi_l\big(x,j(E)\big)$ 在 $\mathbb{F}_p$ 上有相同的因子分解模式. 特别地, 当且仅当 $\Phi_l^c\big(x,j(E)\big)$ 在 $\mathbb{F}_p$ 中有根时, l 为 Elkies 素数.

$\Phi_l^c\big(x,j(E)\big)$ 在 $\mathbb{F}_p$ 上的分解模式是由 (5.2) 式中的 $\overline{f}(x)$ 在 $\mathbb{F}_l$ 上的分解模式所决定的.

定理 5.3　设 d_i 是使 $\phi^{d_i}(C_i)=C_i\,(0\leqslant i\leqslant l)$ 成立的最小正整数, 则

(1) 若 $\overline{f}(x)=(x-\alpha)^2,\quad \alpha\in F_l$, 则对所有 $0\leqslant i\leqslant l$ 有 $d_i=1$, 或者存在一个 j, 使得 $d_j=1$, 而 $d_i=l\quad(0\leqslant i\leqslant l, i\neq j)$, 这时 $t^2\equiv 4p(\mathrm{mod}\ l)$.

(2) 若 $\overline{f}(x)=(x-\alpha)(x-\beta),\quad \alpha,\beta\in F_l^*,\ \ \alpha\neq\beta$, 则存在 $i_1\neq i_2$, 使得 $d_{i_1}=d_{i_2}=1$, 其余的 $d_i=d=\mathrm{ord}(\alpha/\beta)$, 这时 $d|l-1$.

(3) 若 $\overline{f}(x)$ 在 F_l 上不可约, 则对所有 $0\leqslant i\leqslant l,\ \ d_i=d=\mathrm{ord}(\alpha^{l-1})$, 其中 α 为 $\overline{f}(x)$ 在 $F_{l^2}^*$ 中的根, 这时 $d|l+1$.

当 (2) 和 (3) 成立时, $t^2=(\xi+\xi^{-1})^2p$, 其中 ξ 为 F_l(情形 (2)) 或 F_{l^2}(情形 (3)) 中的 d 次本原单位根.

证明　ϕ 在 $E[l]$ 上的作用 ϕ_l 可用一个 2 阶可逆方阵 A 表示, 其特征多项式为 $\overline{f}(x)$.

(1) 这时可取 $A=\begin{pmatrix}\alpha&0\\0&\alpha\end{pmatrix}$ 或 $A=\begin{pmatrix}\alpha&\lambda\\0&\alpha\end{pmatrix}$ $(\lambda\neq0)$. 在前一情形, 对所有 C_i 有 $\phi_l(C_i)=C_i$, 在后一情形有 $A\begin{pmatrix}1\\0\end{pmatrix}=\alpha\begin{pmatrix}1\\0\end{pmatrix}$ 且 $A^l=\begin{pmatrix}\alpha^l&l\alpha\lambda\\0&\alpha^l\end{pmatrix}=\begin{pmatrix}\alpha&0\\0&\alpha\end{pmatrix}$, 故对其余的 C_i 都有 $\phi_l^l(C_i)=C_i$.

(2) 这时可取 $A=\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}$, 这时

$$\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix}=\alpha\begin{pmatrix}1\\0\end{pmatrix},\qquad \begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix}=\beta\begin{pmatrix}0\\1\end{pmatrix},$$

而当 $b_1b_2\neq0$ 时,

$$\begin{pmatrix}\alpha&0\\0&\beta\end{pmatrix}\begin{pmatrix}b_1\\b_2\end{pmatrix}=\beta\begin{pmatrix}\alpha/\beta\cdot b_1\\b_2\end{pmatrix},$$

可见 ϕ_l^d 是恒等映射, 且 d 是所要的最小正整数.

(3) 这时 $\overline{f}(x) = (x-\alpha)(x-\alpha^l)$, $\alpha \in F_{l^2}$, d 是最小正整数, 使得 $\alpha^d = \alpha^{ld}$, 即使 ϕ^d 为恒等映射.

记 α, β 为 A 的两个本征根 (在 (3) 中 $\beta = \alpha^l$), d 是使得 $\alpha^d = \beta^d$ 成立的最小正整数, 因 $\alpha\beta = p$, 故 $\alpha^{2d} = p^d$, $\alpha^2 = \xi_d p$, ξ_d 为 F_l (情形 (2)) 或 F_{l^2} (情形 (3)) 中 d 次本原单位根, 从而

$$t^2 = (\alpha + p/\alpha)^2 = \alpha^2 + p^2/\alpha^2 + 2p = p(\xi_d^2 + \xi_d^{-2} + 2),$$

证毕.

定理 5.3 表明, $\Phi_l^c(x, j(E))$ 在 $\mathbb{F}_p$ 上可能有如下分解模式:

$$(1, l), \quad (1, 1, \cdots, 1), \quad \underset{d|l-1}{(1, 1, d, \cdots, d)}, \qquad \underset{d|l+1}{(d, d, \cdots, d)},$$

在前 3 种情形, l 为 Elkies 素数, 在最后一种情形, l 为 Arkin 素数, 这时

$$t \equiv \pm(\xi_d + \xi_d^{-1})\sqrt{p} \pmod{l}. \tag{5.13}$$

§5.3 计算同种曲线

设 E 为 (5.1) 式定义的椭圆曲线, l 为 Elkies 素数, g 为 $\Phi_l^c(x, j(E))$ 在 $\mathbb{F}_p$ 中的一个根. 由定理 2.5, 存在 $\tau_0 \in \mathfrak{H}$, 使得 $c = -g_2(\tau_0)/4$, $b = -g_3(\tau_0)/4$, $j(E) = j(\tau_0)$, $g = g(\tau_0)$ ($g(\tau)$ 的定义见 (5.4)), 根据已知的 a, b, g, 我们要计算以 $j(l\tau_0)$ 为 j 不变量的 E 的同种椭圆曲线.

定义 $\mathfrak{H}$ 上的函数 ($q = e^{2\pi i \tau}$):

$$\begin{aligned}
E_2(\tau) &= 1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n} = 1 - 24\sum_{n=1}^{\infty}\sigma_1(n)q^n, \\
E_4(\tau) &= 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n} = 1 + 240\sum_{n=1}^{\infty}n^3\sum_{m=1}^{\infty}q^{nm} = 1 + 240\sum_{n=1}^{\infty}\sigma_3(n)q^n, \\
E_6(\tau) &= 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n} = 1 - 504\sum_{n=1}^{\infty}n^5\sum_{m=1}^{\infty}q^{nm} = 1 - 504\sum_{n=1}^{\infty}\sigma_5(n)q^n, \\
\Delta(\tau) &= \frac{E_4(q)^3 - E_6(q)^2}{1728}, \\
j(\tau) &= \frac{E_4^3(\tau)}{\Delta(\tau)} = 1728 + \frac{E_6(\tau)^2}{\Delta(\tau)}.
\end{aligned} \tag{5.14}$$

由 (2.7) 式得

$$g_2(\tau) = \frac{(2\pi)^4}{12}E_4(\tau), \qquad g_3(\tau) = \frac{(2\pi)^6}{6^3}E_6(\tau).$$

设格 $L = \mathbb{Z} + \mathbb{Z}_\tau$, $\tau \in \mathfrak{H}$, 容易验证 $\left(\lambda^{-2}\wp(z, L), \frac{\lambda^{-3}}{2}\wp'(z, L)\right)$ 是曲线

$$E: \quad y^2 = x^3 - 3E_4(\tau)x - 2E_6(\tau) \tag{5.15}$$

上的点, 其中 $\lambda = \frac{\pi}{\sqrt{3}}$, 且 $E \simeq \mathbb{C}/L$, $j(E) = j(\tau)$((2.8) 式). 令 $\widetilde{L} = \mathbb{Z} + \mathbb{Z}_{l\tau}$, 则曲线

$$\widetilde{E}: \quad y^2 = x^3 - 3E_4(l\tau)x - 2E_6(l\tau) \tag{5.16}$$

与 $\mathbb{C}/\widetilde{L}$ 同构, 且 $j(\widetilde{E}) = j(l\tau)$. 又令 $\widehat{L} = (1/l)\widetilde{L} = \mathbb{Z}_{1/l} + \mathbb{Z}_\tau$, 由于

$$\sum_{m,n}{}' \frac{1}{(m\tau + n/l)^{2k}} = l^{2k} \sum_{m,n}{}' \frac{1}{(ml\tau + n)^{2k}},$$

所以曲线

$$\widehat{E}: \quad y^2 = x^3 - 3l^4E_4(l\tau)x - 2l^6E_6(l\tau) \tag{5.17}$$

与 $\mathbb{C}/\widehat{L}$ 同构, $j(\widehat{E})$ 仍为 $j(l\tau)$.

设函数 $f(\tau)$ 是 q 的幂级数, 定义符号 $f'(\tau) = \frac{1}{2\pi i}\frac{df}{d\tau} = q \cdot \frac{df}{dq}$.

引理 5.3

$$\frac{j'(\tau)}{j(\tau)} = -\frac{E_6(\tau)}{E_4(\tau)}, \quad \frac{j'(\tau)}{j(\tau) - 1728} = -\frac{E_4^2(\tau)}{E_6(\tau)}, \quad j'(\tau) = -\frac{E_4^2(\tau)E_6(\tau)}{\Delta(\tau)}.$$

证明 利用命题 2.3, $E_4(\tau)$(权为 4 的模形式) 以 ρ 为惟一零点, 阶为 1. $E_6(\tau)$(权为 6 的模形式) 以 i 为惟一零点, 阶为 1. $j(\tau)$(模函数) 以 ∞ 为惟一极点, 阶为 1, 以 ρ 为惟一零点, 阶为 3.

可见 $j'(\tau)/j(\tau)$ 和 $E_6(\tau)/E_4(\tau)$ 都是权为 2 的模形式, 以 ρ 为惟一极点, 阶为 1. 一定存在常数 c, 使得 $j'(\tau)/j(\tau) - cE_6(\tau)/E_4(\tau)$ 没有极点, 因而恒为常数. 若该常数不是零, 由于 (2.9) 式右端为 1/6, 左端各项为非负, 不可能成立, 故 $j'(\tau)/j(\tau) = cE_6(\tau)/E_4(\tau)$, 比较两端 q 展开式首项系数, 得 $c = -1$.

利用 (5.14) 式可得

$$\frac{j'(\tau)}{j(\tau) - 1728} = \frac{j'(\tau)}{j(\tau)} \cdot \frac{j(\tau)\Delta(\tau)}{E_6^2(\tau)} = -\frac{E_4^2(\tau)}{E_6(\tau)},$$

及

$$j'(\tau) = -\big(j(\tau) - 1728\big)\frac{E_4^2(\tau)}{E_6(\tau)} = -\frac{E_4^2(\tau)E_6(\tau)}{\Delta(\tau)}.$$

证毕.

引理 5.4

$$\frac{\Delta'(\tau)}{\Delta(\tau)}=E_2(\tau),\quad \frac{3E_4'(\tau)}{E_4(\tau)}=E_2(\tau)-\frac{E_6(\tau)}{E_4(\tau)},\quad \frac{2E_6'(\tau)}{E_6(\tau)}=E_2(\tau)-\frac{E_4^2(\tau)}{E_6(\tau)}.$$

证明 熟知

$$\Delta(\tau)=\eta(\tau)^{24}=q\prod_{n\geqslant 1}(1-q^n)^{24},$$

故

$$\frac{\Delta'(\tau)}{\Delta(\tau)}=1-24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}=E_2(\tau).$$

将 $j(\tau)=E_4^3(\tau)/\Delta(\tau)$ 取对数微商, 得

$$\frac{j'(\tau)}{j(\tau)}=\frac{3E_4'(\tau)}{E_4(\tau)}-\frac{\Delta'(\tau)}{\Delta(\tau)}.$$

由引理 3.3 第 1 式得

$$\frac{3E_4'(\tau)}{E_4(\tau)}=E_2(\tau)-\frac{E_6(\tau)}{E_4(\tau)}.$$

将 $j(\tau)-1728=E_6^2(\tau)/\Delta(\tau)$ 取对数微商, 得

$$\frac{j'(\tau)}{j(\tau)-1728}=\frac{2E_6'(\tau)}{E_6(\tau)}-\frac{-\Delta'(\tau)}{\Delta(\tau)},$$

由引理 5.3 第 2 式得

$$\frac{2E_6'(\tau)}{E_6(\tau)}=E_2(\tau)-\frac{E_4^2(\tau)}{E_6(\tau)}.$$

证毕.

引理 5.5 $12E_2'(\tau)=E_2^2(\tau)-E_4(\tau)$.

证明见文献 [12].

由 (5.8) 和 (5.9) 式, 有

$$\Phi_l^c\big(g(\tau),j(\tau)\big)=0. \tag{5.18}$$

由 (5.10) 式, 有

$$\Phi_l^c\big(f(\tau),j(l\tau)\big)=0. \tag{5.19}$$

取 (5.18) 式左端的微商得

$$g'(\tau)\frac{\partial\Phi_l^c}{\partial x}\big(g(\tau),j(\tau)\big)+j'(\tau)\frac{\partial\Phi_l^c}{\partial y}\big(g(\tau),j(\tau)\big)=0.$$

记 $D_g(\tau)=g(\tau)\frac{\partial\Phi_l^c}{\partial x}(g(\tau),j(\tau))$, $D_j(\tau)=j(\tau)\frac{\partial\Phi_l^c}{\partial y}(g(\tau),j(\tau))$, $Z(\tau)=g'(\tau)/g(\tau)$, 利用上式及引理 5.3 得

$$Z(\tau)=-\frac{j'(\tau)}{j(\tau)}\cdot\frac{D_j(\tau)}{D_g(\tau)}=\frac{E_6(\tau)}{E_4(\tau)}\cdot\frac{D_j(\tau)}{D_g(\tau)}. \tag{5.20}$$

令

$$E_0(\tau)=E_6(\tau)/E_4(\tau)Z(\tau), \tag{5.21}$$

则

$$D_j(\tau)E_0(\tau)-D_g(\tau)=0.$$

取上式微商得

$$D_j'(\tau)E_0(\tau)+E_0'(\tau)D_j(\tau)-D_g'(\tau)=0,$$

所以

$$E_0'(\tau)=\big(D_g'(\tau)-D_j'(\tau)E_0(\tau)\big)/D_j(\tau), \tag{5.22}$$

其中

$$D_g'(\tau)=g'(\tau)\frac{\partial\Phi_l^c}{\partial x}(g(\tau),j(\tau))+g(\tau)\Big[g'(\tau)\frac{\partial^2\Phi_l^c}{\partial x^2}(g(\tau),j(\tau))+j'(\tau)\frac{\partial^2\Phi_l^c}{\partial x\partial y}(g(\tau),j(\tau))\Big],$$

$$D_g'(\tau)=j'(\tau)\frac{\partial\Phi_l^c}{\partial y}(g(\tau),j(\tau))+j(\tau)\Big[j'(\tau)\frac{\partial^2\Phi_l^c}{\partial y^2}(g(\tau),j(\tau))+g'(\tau)\frac{\partial^2\Phi_l^c}{\partial x\partial y}(g(\tau),j(\tau))\Big],$$

而 $g'(\tau)$ 和 $j'(\tau)$ 可由下式给定：

$$g'(\tau)=Z(\tau)g(\tau),\qquad j'(\tau)=-j(\tau)E_6(\tau)/E_4(\tau).$$

由于

$$g(\tau)=l^s\left(\frac{\eta(l\tau)}{\eta(\tau)}\right)^{2s},$$

故

$$Z(\tau)=2s\Big(\frac{l\eta'(l\tau)}{\eta(l\tau)}-\frac{\eta'(\tau)}{\eta(\tau)}\Big)=\frac{s}{12}\big(lE_2(l\tau)-E_2(\tau)\big)\quad(\text{引理 5.4 及}\Delta=\eta^{24}), \tag{5.23}$$

及 (引理 5.5)

$$Z'(\tau)=\frac{s}{12}(l^2E_2'(l\tau)-E_2'(\tau))=\frac{s}{12^2}[l^2\big(E_2^2(l\tau)-E_4(l\tau)\big)-\big(E_2^2(\tau)-E_4(\tau)\big)],$$

从而

$$\begin{aligned}
l^2E_4(l\tau) =& E_4(\tau) + l^2E_2^2(l\tau) - E_2^2(\tau) - \frac{12^2}{s}Z'(\tau)\\
=& E_4(\tau) + \big(lE_2(l\tau) - E_2(\tau)\big)\big(lE_2(l\tau) - E_2(\tau) + 2E_2(\tau)\big)\\
&+ \frac{12Z(\tau)}{s}\left(\frac{12E_0'(\tau)}{E_0(\tau)} + \frac{12E_4'(\tau)}{E_4(\tau)} - \frac{12E_6'(\tau)}{E_6(\tau)}\right)\\
=& E_4(\tau) + \frac{12Z(\tau)}{s}\left(\frac{12Z(\tau)}{s} + 2E_2(\tau)\right)\\
&+ \frac{12Z(\tau)}{s}\left(\frac{12E_0'(\tau)}{E_0(\tau)} + 4E_2(\tau) - \frac{4E_6(\tau)}{E_4(\tau)} - 6E_2(\tau) + \frac{6E_4^2(\tau)}{E_6(\tau)}\right)\\
=& E_4(\tau) + \frac{12Z(\tau)}{s}\left(\frac{12E_0'(\tau)}{E_0(\tau)} + \frac{6E_4^2(\tau)}{E_6(\tau)} - \frac{4E_6(\tau)}{E_4(\tau)} + \frac{12Z(\tau)}{s}\right), \qquad (5.24)
\end{aligned}$$

其中利用了引理 5.4 及由 (5.21) 式可推出的

$$\frac{Z'(\tau)}{Z(\tau)} = \frac{E_6'(\tau)}{E_6(\tau)} - \frac{E_4'(\tau)}{E_4(\tau)} - \frac{E_0'(\tau)}{E_0(\tau)}.$$

将 (5.19) 式左端取微商得到

$$f'(\tau)\frac{\partial \Phi_l^c}{\partial x}\big(f(\tau), j(l\tau)\big) + lj'(l\tau)\frac{\partial \Phi_l^c}{\partial y}\big(f(\tau), j(l\tau)\big) = 0,$$

从而

$$\frac{E_6(l\tau)}{E_4(l\tau)} = -\frac{j'(l\tau)}{j(l\tau)} = f'(\tau)\frac{\partial \Phi_l^c}{\partial x}\big(f(\tau), j(l\tau)\big)/lj(l\tau)\frac{\partial \Phi_l^c}{\partial y}\big(f(\tau), j(l\tau)\big), \qquad (5.25)$$

由于 $f(\tau) = l^s/g(\tau)$, 故

$$f'(\tau) = -\frac{f(\tau)g'(\tau)}{g(\tau)} = -f(\tau)Z(\tau), \qquad (5.26)$$

而

$$j(l\tau) = \frac{E_4^3(l\tau)}{\Delta(l\tau)}, \qquad \Delta(l\tau) = \frac{\Delta(\tau)g(\tau)^{12/s}}{l^{12}}, \qquad (5.27)$$

利用 (5.24)~(5.27) 式可得到 $E_6(l\tau)$.

给定曲线

$$E: \quad y^2 = x^3 + ax + b,$$

利用方程 (5.15), 存在 $\tau_0 \in \mathfrak{H}$, 使得

$$E_4(\tau_0) = -a/3, \qquad E_6(\tau_0) = -b/2.$$

我们要计算由方程 (5.17) 决定的 E 的同种曲线

$$\widehat{E}: \quad y^2 = x^3 + \widehat{a}x + \widehat{b}, \tag{5.28}$$

其中

$$\widehat{a} = -3l^4 E_4(l\tau_0), \quad \widehat{b} = -2l^6 E_6(l\tau_0).$$

为了方便, 下文中对任一函数 $f(\tau)$, 用 f 表示 $f(\tau_0)$, 用 $f^{(l)}$ 表示 $f(l\tau_0)$, 所以给定 a, b 后, 我们有

$$\begin{aligned} &E_4 = -a/3, \qquad E_6 = -b/2, \qquad \Delta = 1728^{-1}(E_4^3 - E_6^2), \\ &j = E_4^3/\Delta, \qquad \Delta^{(l)} = \Delta \cdot g^{12/s}/l^{12}, \end{aligned}$$

其中 g 是 $\Phi_l^c(x, j)$ 在 $\mathbb{F}_p$ 中的根.

当 $D_j \neq 0$ 时, 利用 (5.20)~(5.22)、(5.24)、(5.25) 式可以算出 $E_4^{(l)}$ 和 $E_6^{(l)}$, 从而得到 $\widehat{a}$ 和 $\widehat{b}$.

当 $D_j = 0$ 时, 由 (5.20) 式得 $Z = 0$, 从而 $E_4^{(l)} = E_4/l^2$((5.24) 式), 这时 $\widehat{a} = -3l^4 E_4^{(l)}$, $j^{(l)} = (E_4^{(l)})^3/\Delta^{(l)}$, $\widehat{b} = \pm 2l^6\sqrt{(j^{(l)} - 1728)\Delta^{(l)}}$ ((5.14) 式).

算法 5.3 中计算 $\widehat{a}$ 和 $\widehat{b}$ 的部分即为本节的方法, 其中用了符号 $E_2^* = -\frac{12}{s}Z$.

§5.4　计算除子多项式的因子

在 §5.3 中提到 $\left(\lambda^{-2}\wp(z, L), \frac{\lambda^{-3}}{2}\wp'(z, L)\right)$ $\left(\lambda = \frac{\pi}{\sqrt{3}}\right)$ 是由 (5.15) 式所定义的曲线 E 上的点, 由 $\wp(z, L)$ 的定义易知

$$\lambda^{-2}\wp(z, L) = \wp(\lambda z, \lambda L), \qquad \lambda^{-3}\wp'(z, L) = \wp'(\lambda z, \lambda L),$$

所以 E 也可看作与格 λL 对应的椭圆曲线, 实际上由 (2.7) 式,

$$\begin{aligned} 3E_4(\tau) &= \frac{3 \cdot 12}{(4\pi)^4} g_2(\tau, L) = \frac{9}{4\pi^4} g_2(\lambda\tau, \lambda L)\lambda^4 = \frac{g_2(\lambda\tau, \lambda L)}{4} = 15 \sum_{\omega \in \lambda L} \omega^{-4}, \\ 2E_6(\tau) &= \frac{2 \cdot 6^3}{(2\pi)^6} g_3(\tau, L) = \frac{3^3}{4\pi^6} g_3(\lambda\tau, \lambda L)\lambda^6 = \frac{g_3(\lambda\tau, \lambda L)}{4} = 35 \sum_{\omega \in \lambda L} \omega^{-6}. \end{aligned} \tag{5.29}$$

本节将计算多项式

$$h(x) = \prod_{k=1}^{(l-1)/2} \left(x - \wp\Big(\frac{k\lambda}{l}, \lambda L\Big)\right),$$

即 $E[l]$ 中对应子空间 $\mathcal{C}_0$ 中的点的 x 坐标所适合的方程, 它是推论 2.3 中的除子多项式 $\phi_l(x)$ 的因子.

引理 5.6

$$\sum_{n=1}^{\infty} \frac{x^n}{(1-x^n)^2} = \sum_{n=1}^{\infty} \sigma_1(n) x^n.$$

证明 将

$$\frac{1}{1-x^n} = \sum_{k=0}^{\infty} x^{nk}$$

两端微商后乘 x^n 得

$$\frac{x^n}{(1-x^n)^2} = \sum_{k=1}^{\infty} k x^{nk},$$

从而

$$\sum_{n=1}^{\infty} \frac{x^n}{(1-x^n)^2} = \sum_{n=1}^{\infty}\sum_{k=1}^{\infty} k x^{nk} = \sum_{n=1}^{\infty} \sigma_1(n) x^n.$$

证毕.

引理 5.7 *设 μ_l 为 l 次单位根集合, 则*

$$\sum_{\xi\in\mu_l} \frac{\xi x}{(1-\xi x)^2} = \frac{l^2 x^l}{(1-x^l)^2}, \quad \sum_{\xi\in\mu_l,\,\xi\neq 1} \frac{\xi}{(1-\xi)^2} = \frac{1-l^2}{12}.$$

证明 我们有

$$\sum_{\xi\in\mu_l} \frac{1}{1-\xi x} = \sum_{\xi\in\mu_l}\sum_{i=0}^{\infty} \xi^i x^i = \sum_{i=0}^{\infty}\Big(\sum_{\xi\in\mu_l}\xi^i\Big) x^i = l\sum_{i=0}^{\infty} x^{il} = \frac{l}{1-x^l},$$

两端微商后乘 x 即得第一式.

由第一式得

$$\sum_{\xi\in\mu_l,\xi\neq 1} \frac{\xi}{(1-\xi x)^2} = \frac{l^2 x^{l-1}}{(1-x^l)^2} - \frac{1}{(1-x)^2} = \frac{l^2 x^{l-1} - \left(\sum_{i=0}^{l-1} x^i\right)^2}{(1-x^l)^2}.$$

当 $x \to 1$ 时, 上式左端的极限即为第二式的左端, 右端极限为

$$
\begin{aligned}
&\lim_{x\to 1}\frac{l^2(l-1)x^{l-2}-2\sum_{i=0}^{l-1}x^i\cdot\sum_{i=0}^{l-2}(i+1)x^i}{2l(x^{2l-1}-x^{l-1})}\\
=&\lim_{x\to 1}\frac{l^2(l-1)(l-2)x^{l-3}-2\Big(\sum_{i=0}^{l-2}(i+1)x^i\Big)^2-2\sum_{i=0}^{l-1}x^i\sum_{i=1}^{l-2}i(i+1)x^{i-1}}{2l\big((2l-1)x^{2l-2}-(l-1)x^{l-2}\big)}\\
=&\frac{1}{2l^2}\Big(l^2(l-1)(l-2)-\frac{1}{2}l^2(l-1)^2\\
&-2l\Big(\frac{(l-2)(l-1)(l-3)}{6}+\frac{(l-1)(l-2)}{2}\Big)\Big)\\
=&\frac{1-l^2}{12}.
\end{aligned}
$$

证毕.

引理 5.8　设 $L=\mathbb{Z}+\mathbb{Z}_\tau$, $q_\tau=e^{2\pi i\tau}$, $q_z=e^{2\pi iz}$, 则

$$
\frac{1}{(2\pi i)^2}\wp(z,L)=\frac{1}{12}+\sum_{n\in\mathbb{Z}}\frac{q_\tau^n q_z}{(1-q_\tau^n q_z)^2}-2\sum_{n=1}^{\infty}\frac{q_\tau^n}{1-q_\tau^n}.
$$

证明　利用

$$
\sin\pi z=\pi z\prod_{n=1}^{\infty}\Big(1-\frac{z}{n}\Big)\Big(1+\frac{z}{n}\Big),
$$

两端取对数微商得

$$
\pi\frac{\cos\pi z}{\sin\pi z}=\frac{1}{z}+\sum_{n=1}^{\infty}\Big(\frac{1}{z-n}+\frac{1}{z+n}\Big),
$$

另一方面,

$$
\pi\frac{\cos\pi z}{\sin\pi z}=\pi i\frac{e^{z\pi i}+e^{-z\pi i}}{e^{z\pi i}-e^{-z\pi i}}=\pi i\frac{q_z+1}{q_z-1}=\pi i+\frac{2\pi i}{q_z-1}=\pi i-2\pi i\sum_{n=0}^{\infty}q_z^n,
$$

所以

$$
\sum_{n\in\mathbb{Z}}\frac{1}{z+n}=\pi i-2\pi i\sum_{n=1}^{\infty}q_z^n,
$$

两端取微商得

$$
\sum_{n\in\mathbb{Z}}\frac{1}{(z+n)^2}=(2\pi i)^2\sum_{n=1}^{\infty}nq_z^n=(2\pi i)^2\frac{q_z}{(1-q_z)^2},
$$

从而

$$\begin{aligned}\wp(z,L)&=\frac{1}{z^2}+\sum_{m,n}{}'\left(\frac{1}{(z+m\tau+n)^2}-\frac{1}{(m\tau+n)^2}\right)\\&=\sum_{m,n}\frac{1}{(z+m\tau+n)^2}-2\sum_{n=1}^{\infty}\frac{1}{n^2}-2\sum_{m=1}^{\infty}\sum_{n\in\mathbb{Z}}\frac{1}{(m\tau+n)^2}\\&=-\frac{\pi^2}{3}+(2\pi i)^2\sum_{m\in\mathbb{Z}}\frac{q_\tau^m q_z}{(1-q_\tau^m q_z)^2}-2(2\pi i)^2\sum_{m=1}^{\infty}\frac{q_\tau^m}{(1-q_\tau^m)^2}.\end{aligned}$$

证毕.

记 $h(x)=x^{\frac{l-1}{2}}+a_{\frac{l-3}{2}}x^{\frac{l-3}{2}}+\cdots+a_1x+a_0$(令 $a_{\frac{l-1}{2}}=1$), 则

$$\begin{aligned}-a_{\frac{l-3}{2}}&=\sum_{k=1}^{\frac{l-1}{2}}\wp\Big(\frac{k\lambda}{l},\lambda L\Big)=\frac{3}{\pi^2}\sum_{k=1}^{\frac{l-1}{2}}\wp\Big(\frac{k}{l},L\Big)=\frac{3}{2\pi^2}\sum_{k=1}^{l-1}\wp\Big(\frac{k}{l},L\Big)\\&=(-6)\left(\frac{l-1}{12}+\sum_{\xi\in\mu_l,\xi\neq1}\sum_{n\in\mathbb{Z}}\frac{\xi q_\tau^n}{(1-\xi q_\tau^n)^2}-2(l-1)\sum_{n=1}^{\infty}\frac{q_\tau^n}{(1-q_\tau^n)^2}\right)\quad(\text{引理 }5.8)\\&=(-6)\left(\frac{l-1}{12}+\sum_{\xi\in\mu_l,\xi\neq1}\frac{\xi}{(1-\xi)^2}+2\sum_{n=1}^{\infty}\sum_{\xi\in\mu_l}\frac{\xi q_\tau^n}{(1-\xi q_\tau^n)^2}-2l\sum_{n=1}^{\infty}\frac{q_\tau^n}{(1-q_\tau^n)^2}\right)\\&=\frac{-l}{2}\left(1-24\sum_{n=1}^{\infty}\frac{q_\tau^n}{(1-q_\tau^n)^2}-l\left(1-24\sum_{n=1}^{\infty}\frac{q_{l\tau}^n}{(1-q_{l\tau}^n)^2}\right)\right)\quad(\text{引理 }5.7)\\&=\frac{l}{2}\left(l\left(1-24\sum_{n=1}^{\infty}\sigma_1(n)q_\tau^{ln}\right)-\left(1-24\sum_{n=1}^{\infty}\sigma_1(n)q_\tau^n\right)\right)\quad(\text{引理 }5.6)\\&=\frac{l}{2}\big(lE_2(l\tau)-E_2(\tau)\big)=\frac{6l}{s}Z(\tau).\quad((5.23)\text{式})\end{aligned}$$

当曲线 E 给定后, $Z=Z(\tau_0)$ 已在算法 5.3 中得到, 其中将 $-a_{\frac{l-3}{2}}$ 记为 p_1.

考虑 $\wp(z,L)$ 关于 z 的幂级数展开式

$$\begin{aligned}\wp(z,L)&=\frac{1}{z^2}+\sum_{\omega\in L}{}'\left(\frac{1}{(z+\omega)^2}-\frac{1}{\omega^2}\right)\\&=\frac{1}{z^2}+\sum_{k=1}^{\infty}(2k+1)\sum_{\omega\in L}{}'\omega^{-(2k+2)}z^{2k}\\&=\frac{1}{z^2}+\sum_{k=1}^{\infty}c_kz^{2k},\end{aligned}$$

其中

$$\begin{aligned} c_1 &= 3\sum_{\omega\in L}{}'\omega^{-4} = \frac{1}{20}g_2(\tau, L) = -\frac{a}{5}, \\ c_2 &= 5\sum_{\omega\in L}{}'\omega^{-6} = \frac{1}{28}g_3(\tau, L) = -\frac{b}{7}, \end{aligned} \tag{5.30}$$

当 $k \geqslant 3$ 时, 利用递推公式

$$c_k = \frac{3}{(k-2)(2k+3)}\sum_{j=1}^{k-2} c_j c_{k-1-j},$$

可以计算所有的 c_k.

定义 ζ 函数

$$\zeta(z) = \zeta(z, L) = \frac{1}{z} - \sum_{k=1}^{\infty}\frac{c_k}{2k+1}z^{2k+1},$$

易见 $\zeta'(z) = -\wp(z)$.

引理 5.9　对任一 $a \in \mathbb{C}\,(a \notin L)$, 有

$$\zeta(z+a) + \zeta(z-a) - 2\zeta(z) = \frac{\wp'(z)}{\wp(z) - \wp(a)}. \tag{5.31}$$

证明　上式两端之差的微商为

$$-\wp(z+a) - \wp(z-a) + 2\wp(z) - \frac{\wp''(z)\big(\wp(z) - \wp(a)\big) - \big(\wp'(z)\big)^2}{\big(\wp(z) - \wp(a)\big)^2}, \tag{5.32}$$

今证该椭圆函数没有极点.

(5.32) 式在 $z = 0$ 的展开式为

$$\begin{aligned} & -2\wp(a) + \frac{2}{z^2} - \Big(\frac{6}{2^4} + O(1)\Big)\Big(\frac{1}{z^2} - \wp(a) + O(z^2)\Big)^{-1} \\ & + \Big(\frac{-2}{z^3} + O(z)\Big)^2\Big(\frac{1}{z^2} - \wp(a) + O(z^2)\Big)^{-2} \\ = & -2\wp(a) + \frac{2}{z^2} - \Big(\frac{6}{z^2} + O(z^2)\Big)\Big(1 + \wp(a)z^2 + O(z^4)\Big) \\ & + \Big(\frac{4}{z^2} + O\Big(\frac{1}{z^2}\Big)\Big)(1 + z\wp(a)z^2 + O(z^4)) \\ = & \, O(z^2), \end{aligned} \tag{5.33}$$

这里 $O(z^k)$ 表示首项次数为 k 的幂级数.

当 $2a \notin L$ 时 (这时 $\wp'(a) \neq 0$), (5.32) 式在 $z = a$ 的展开式为

$$
\begin{aligned}
&-\frac{1}{(z-a)^2} - \big(\wp''(a) + O(z-a)\big)\big(\wp'(a)(z-a) + O((z-a)^2)\big)^{-1} \\
&+ \big(\wp'(a) + \wp''(a)(z-a) + O((z-a)^2)\big)^2 \Big(\wp'(a)(z-a) \\
&+ \frac{\wp''(a)}{2}(z-a)^2 + O((z-a)^3)\Big)^{-2} + O(1) \\
=& -\frac{1}{(z-a)^2} - \frac{\wp''(a)}{\wp'(a)} \cdot \frac{1}{z-a} + \Big(\frac{1}{(z-a)^2} + \frac{2\wp''(a)}{\wp'(a)(z-a)} + O(1)\Big) \\
&\times \Big(1 + \frac{\wp''(a)(z-a)}{2\wp'(a)} + O((z-a)^2)\Big)^{-2} + O(1) \\
=& -\frac{1}{(z-a)^2} - \frac{\wp''(a)}{\wp'(a)} \cdot \frac{1}{z-a} + \Big(\frac{1}{(z-a)^2} + \frac{2\wp''(a)}{\wp'(a)(z-a)} + O(1)\Big) \\
&\times \Big(1 - \frac{\wp''(a)(z-a)}{\wp'(a)}\Big) + O(1) \\
=& \, O(1).
\end{aligned}
$$

当 $2a \in L$ 时 (这时 $\wp'(a) = 0$, $\wp''(a) \neq 0$), (5.32) 式在 $z = a$ 的展开式为

$$
-\frac{2}{(z-a)^2} - \big(\wp''(a) + O(z-a)\big)\Big(\frac{\wp''(a)}{2}(z-a)^2 + O((z-a)^3)\Big)^{-1} + O(1) = O(1).
$$

类似地可证明 (5.32) 式在 $z = -a$ 的展开式亦为 $O(1)$, 因而 (5.32) 式是一个常数. 当 $z = 0$ 时该函数取值为零, 可见 (5.32) 式恒为零, 从而 (5.31) 等式两端之差是一个常数. 该差在 $z = 0$ 的展开式为 (注意 $\zeta(-a) = -\zeta(a)$)

$$
-\frac{2}{z} - \Big(\frac{-2}{z^3} + O(z)\Big)\Big(\frac{1}{z^2} + O(1)\Big)^{-1} + O(z) = O(z).
$$

可见 (5.31) 式两端之差为零, 证毕.

记 $\widehat{L} = \mathbb{Z}_{1/l} + \mathbb{Z}_\tau$ 及

$$
\widehat{\wp}(z) = \wp(z, \lambda\widehat{L}) = \frac{1}{z^2} + \sum_{k=1}^{\infty} \widehat{c}_k z^{2k}, \qquad \widehat{\zeta}(z) = \frac{1}{z} - \sum_{k=1}^{\infty} \frac{\widehat{c}_k}{2k+1} z^{2k+1}.
$$

我们有 ((5.28) 式, (5.30) 式)

$$
\widehat{c}_1 = -\widehat{a}/5, \quad \widehat{c}_2 = -\widehat{b}/7.
$$

$\widehat{a}, \widehat{b}$ 已在算法 5.3 中得到.

引理 5.10

(i) $\widehat{\wp}(z)=\sum_{i=0}^{l-1}\wp\big(z+\frac{i\lambda}{l}\big)-\sum_{i=1}^{l-1}\wp\big(\frac{i\lambda}{l}\big)$,

(ii) $\sum_{-l/2<i<l/2}\zeta\big(z+\frac{i\lambda}{l}\big)=\widehat{\zeta}(z)-z\sum_{i=1}^{l-1}\wp\big(\frac{i\lambda}{l}\big)$.

证明　(i) 考虑函数

$$\widehat{\wp}(z)-\sum_{i=0}^{l-1}\wp\Big(z+\frac{i\lambda}{l}\Big),$$

它以 $\lambda\widehat{L}$ 为周期, 且没有极点, 故是一个常数. 当 $z=0$ 时上述函数取值为

$$-\sum_{i=1}^{l-1}\wp\Big(\frac{i\lambda}{l}\Big),$$

(ii) 函数

$$\sum_{-l/2<i<l/2}\zeta\Big(z+\frac{i\lambda}{l}\Big)-\widehat{\zeta}(z)$$

的微商是

$$\widehat{\wp}(z)-\sum_{-l/2<i<l/2}\wp\Big(z+\frac{i\lambda}{l}\Big),$$

利用 (i) 可知

$$\sum_{-l/2<i<l/2}\zeta\Big(z+\frac{i\lambda}{l}\Big)-\widehat{\zeta}(z)+z\sum_{i=1}^{l-1}\wp\Big(\frac{i\lambda}{l}\Big)$$

是一个常数. 当 $z=0$ 时上式取值为零, 证毕.

定理 5.4

$$z^{l-1}h\big(\wp(z)\big)=\exp\Bigg(-p_1z^2-\sum_{k=1}^{\infty}\frac{\widehat{c}_k-lc_k}{(2k+1)(2k+2)}z^{2k+2}\Bigg).$$

证明　由引理 5.9 有 $\Big(i=1,2,\cdots,\frac{l-1}{2}\Big)$

$$\zeta\Big(z+\frac{i}{l}\lambda\Big)+\zeta\Big(z-\frac{i}{l}\lambda\Big)-2\zeta(z)=\frac{\wp'(z)}{\wp(z)-\wp\Big(\dfrac{i\lambda}{l}\Big)},$$

将诸式相加得

$$-l\zeta(z)+\sum_{-l/2<l<l/2}\zeta\Big(z+\frac{i\lambda}{l}\Big)=\sum_{i=1}^{(l-1)/2}\frac{\wp'(z)}{\wp(z)-\wp\Big(\dfrac{i\lambda}{l}\Big)}.$$

利用引理 5.10 的 (ii),

$$-l\zeta(z)+\widehat{\zeta}(z)-2p_1z=\sum_{i=1}^{(l-1)/2}\frac{\wp'(z)}{\wp(z)-\wp\left(\frac{i\lambda}{l}\right)},$$

上式即为

$$\frac{1-l}{z}-\sum_{k=1}^{\infty}\frac{\widehat{c}_k-lc_k}{2k+1}z^{2k+1}-2p_1z=\sum_{i=1}^{(l-1)/2}\frac{\wp'(z)}{\wp(z)-\wp\left(\frac{i\lambda}{l}\right)},$$

从而

$$z^{1-l}\exp\left(-p_1z^2-\sum_{k=1}^{\infty}\frac{\widehat{c}_k-lc_k}{(2k+1)(2k+2)}z^{2k+2}\right)=c\prod_{i=1}^{(l-1)/2}\left(\wp(z)-\wp\left(\frac{i\lambda}{l}\right)\right),$$

其中 c 为一常数. 比较等式的两端展开式中 z^{1-l} 项的系数, 可知 $c=1$, 证毕.

利用定理 5.4 可以计算 $h(x)$ 的系数 (算法 5.4).

我们有

$$\begin{aligned}&z^{1-l}\exp\left(-p_1z^2-\sum_{k=1}^{\infty}\frac{\widehat{c}_k-lc_k}{(2k+1)(2k+2)}z^{2k+2}\right)\\=\;&z^{1-l}\sum_{r=0}^{\infty}\frac{1}{r!}\left(-p_1z^2-\sum_{k=1}^{\infty}\frac{\widehat{c}_k-lc_k}{(2k+1)(2k+2)}z^{2k+2}\right)^r\\=\;&z^{1-l}\sum_{r=0}^{\infty}d_rz^{2r},\end{aligned}$$

仅需计算 $d_0,d_1,\cdots,d_{(l-1)/2}$. 另一方面

$$\begin{aligned}h\big(\wp(z)\big)&=\sum_{i=0}^{(l-1)/2}a_{(l-1)/2-i}\left(\frac{1}{z^2}+\sum_{k=1}^{\infty}c_kz^{2k}\right)^{\frac{l-1}{2}-i}\\&=z^{1-l}\sum_{i=0}^{(l-1)/2}a_{(l-1)/2-i}\sum_{j=0}^{(l-1)/2-i}b_{(l-1)/2-i,j}z^{2(i+j)}+O(z^2)\\&=z^{1-l}\sum_{r=0}^{(l-1)/2}\left(\sum_{i=0}^{r}a_{(l-1)/2-i}b_{(l-1)/2-i,r-i}\right)z^{2r}+O(z^2),\end{aligned}$$

其中

$$\left(1+\sum_{k=1}^{\infty}c_kz^{2k+2}\right)^{\frac{l-1}{2}-i}=\sum_{j=0}^{\frac{l-1}{2}-i}b_{\frac{l-1}{2}-i,j}z^{2j}+\cdots$$

对任意 i, 有 $b_{(l-1)/2-i,0}=1$, $b_{(l-1)/2-i,1}=0$. 利用

$$d_r=\sum_{i=0}^{r}a_{(l-1)/2-i}b_{(l-1)/2-i,r-i},\qquad r=2,3,\cdots,\frac{l-1}{2}$$

可以依次计算 $a_{(l-5)/2},a_{(l-7)/2},\cdots,a_0$.

利用 $h(x)$, 寻找 $\alpha\,(1\leqslant\alpha\leqslant l)$, 使得

$$\begin{aligned}(x^p,y^p)&\equiv\alpha(x,y)\\&\equiv\left(x-\frac{\psi_{\alpha-1}\cdot\psi_{\alpha+1}}{\psi_\alpha^2},\frac{\psi_{\alpha+2}\cdot\psi_{\alpha-1}^2-\psi_{\alpha-2}\cdot\psi_{\alpha+1}^2}{4y\psi_\alpha^3}\right)\\&\quad(\mathrm{mod}\ h(x),y^2-x^3-ax-b)\end{aligned}$$

(定理 2.11). 由于 $-\alpha=\alpha(x,-y)$, 仅需在区间 $[1,(l-1)/2]$ 中寻找 α(算法 5.5).

§5.5 Atkin 算法

在 §5.2 中我们已指出 $\Phi_l^c(x,j(E))$ 在 $\mathbb{F}_p$ 中有 4 种可能的分解模式:

$$(1,l),\quad(1,1,\cdots,1),\quad\underset{d|l-1}{(1,1,d,\cdots,d)},\qquad\underset{d|l+1}{(d,d,\cdots,d)},$$

令

$$d_1=\deg\left(\gcd(x^p-x,\Phi_l^c(x,j(E)))\right).$$

若 $d_1=1$, 则 $\Phi_l^c(x,j(E))$ 的分解模式为 $(1,l)$. (5.2) 式中 $\overline{f}(x)$ 的本征根 α 适合 $\alpha^2\equiv p\ (\mathrm{mod}\ l)$, 故 $t\equiv\pm2\sqrt{p}\ (\mathrm{mod}\ l)$.

若 $d_1=l+1$, 则 $\Phi_l^c(x,j(E))$ 的分解模式为 $(1,1,\cdots,1)$, 这时对任一 $Q\in E[l]$, 都有 $\phi(Q)=\alpha(Q)$, 我们有更进一步的结果.

命题 5.2 *若对任一 $Q\in E[l]$, 都有 $\phi(Q)=\alpha Q\,(1<\alpha<l)$, 则 $t\equiv\alpha+p\alpha^{-1}$ $(\mathrm{mod}\ l^2)$.*

证明 对任一 $P\in E[l^2]$, 由于 $lP\in E[l]$, 故 $\phi(lP)=\alpha lP$, 于是 $l(\phi(P)-\alpha P)=\mathcal{O}$. 令 $T=\phi(P)-\alpha P\in E[l]$, 则有

$$\begin{aligned}\mathcal{O}&=\phi^2(P)-t\phi(P)+pP\\&=\phi(\alpha P+T)-t(\alpha P+T)+pP\\&=\alpha^2P+2\alpha T-t(\alpha P+T)+pP\\&=(\alpha^2-t\alpha+p)P,\end{aligned}$$

这里利用了 $t\equiv2\alpha\ (\mathrm{mod}\ l)$, 可见 $\alpha^2-t\alpha+p\equiv0\ (\mathrm{mod}\ l^2)$, 证毕.

关于 $\Phi_l^c(x,j(E))$ 在 $\mathbb{F}_p$ 上的素因子个数, 有如下的结果:

命题 5.3 设 E 在 $\mathbb{F}_p$ 上非超奇异, 且 $j(E) \neq 0, 1728$, l 为奇素数, s 为 $\Phi_l^c(x, j(E))$ 在 $\mathbb{F}_p$ 上的不可约因子个数, 则

$$(-1)^s = \left(\frac{p}{l}\right).$$

证明 分别考虑定理 5.3 中的 3 个情形.

(1) $\overline{f}(x) = (x-\alpha)^2, \alpha \in \mathbb{F}_l$, 这时 $\Phi_l^c(x, j(E))$ 的分解模式为 $(1, l)$ 或 $(1, 1, \cdots, 1)$, s 为偶数, 由于 $t^2 \equiv 4p \pmod l$, 故 $\left(\frac{p}{l}\right) = 1$.

(2) $\overline{f}(x) = (x-\alpha)(x-\beta)$, $\alpha, \beta \in \mathbb{F}_l^*$, $\alpha \neq \beta$, 这时 $\Phi_l^c(x, j(E))$ 的分解模式为 $(1, 1, d, \cdots, d)$, $s \equiv (l-1)/d \pmod 2$, d 为 α/β 在 $\mathbb{F}_l^*$ 中的阶, 当且仅当 $(l-1)/d$ 为偶数时, $\alpha/\beta \in (\mathbb{F}_l^*)^2$. 由于 $p = \alpha\beta = \beta^2 \cdot \alpha/\beta$, 故当且仅当 s 为偶数时, $p \in (\mathbb{F}_l^*)^2$.

(3) $\overline{f}(x) = (x-\alpha)(x-\alpha^l)$, $\alpha \in \mathbb{F}_{l^2}^*$, 这时 $\Phi_l^c(x, j(E))$ 的分解模式为 $(d, d, \cdots, d)$, $s = (l+1)/d$, d 为 α^{l-1} 在 $\mathbb{F}_{l^2}^*$ 中的阶, 令 ζ 为 $\mathbb{F}_{l^2}^*$ 的原根, 则 ζ^{l+1} 为 $\mathbb{F}_l^*$ 的原根. 设 $\alpha = \zeta^r$, 则 $p = \alpha^{l+1} = \left(\zeta^{l+1}\right)^r$, 所以当且仅当 r 为偶数时 $p \in \left(\mathbb{F}_{l^2}^*\right)^2$. 由于 $\alpha^{l-1} = \zeta^{r(l-1)}$, 故

$$d = \frac{l^2-1}{((l^2-1), r(l-1))} = \frac{l+1}{(l+1, r)},$$

即

$$(l+1, r) = \frac{l+1}{d} = s,$$

当且仅当 s 为偶数时, r 亦为偶数, 证毕.

上述 Atkin 算法见算法 5.6, 其中利用 (5.13) 式给出几个可能的 $t \bmod l$ 的值.

利用 SEA 算法可能得到一组 $t \bmod l$ 的值, 然后利用中国剩余定理, 可以得到 $t\,(\leqslant \sqrt{2p})$. 具体计算时, 我们利用下述小步 – 大步算法 (见算法 5.7).

假设

$$\begin{aligned} t &\equiv c_1 \mod m_1, \quad c_1 \in \mathcal{C}_1, \\ t &\equiv c_2 \mod m_2, \quad c_2 \in \mathcal{C}_2, \\ t &\equiv c_3 \mod m_3, \end{aligned} \tag{5.34}$$

这里 m_1, m_2, m_3 两两互素, 且 $m_1m_2m_3 > 4\sqrt{p}$, c_1 和 c_2 分别取自已知的集合 $\mathcal{C}_1$ 和 $\mathcal{C}_2$. 令

$$\begin{aligned} r_2 &\equiv (c_2 - c_3)(m_1m_3)^{-1} \pmod{m_2}, \\ r_1 &\equiv (c_1 - c_3)(m_2m_3)^{-1} \pmod{m_1}, \end{aligned}$$

易见

$$t = c_3 + m_3(m_1r_2 + m_2r_1) \tag{5.35}$$

是 (5.34) 式的一个解, 显然我们要求 $|t| \leqslant 2\sqrt{p}$.

命题 5.4 假设在 (5.35) 式中有 $|t| \leqslant 2\sqrt{p}, 0 \leqslant c_3 < m_3, |r_1| \leqslant m_1/2, m_1m_2m_3 > 4\sqrt{p}$, 则 $|r_2| \leqslant m_2$.

证明 由于

$$r_2 = \frac{1}{m_1m_3}(t - c_3 - m_2m_3r_1),$$

从而

$$|r_2| \leqslant \frac{2\sqrt{p}}{m_1m_3} + \frac{1}{m_1} + \frac{m_2}{2} < \frac{m_2}{2} + \frac{1}{m_1} + \frac{m_2}{2} = m_2 + \frac{1}{m_1},$$

因 r_2 为整数, 故 $|r_2| \leqslant m_2$, 证毕.

任取 $c_1 \in \mathcal{C}_1, c_2 \in \mathcal{C}_2$, 分别得到 r_1 和 r_2, 使它们满足 $|r_1| \leqslant m_1/2, |r_2| \leqslant m_2$, 利用 (5.35) 式得到 $\#E(\mathbb{F}_p)$ 的一个可能值

$$h = p + 1 - \big(c_3 + m_3(m_1r_2 + m_2r_1)\big),$$

为了验证 h 是否就是 $\#E(\mathbb{F}_p)$, 任取 $P \in E(\mathbb{F}_p)$, 验算 $hP = \mathcal{O}$ 是否成立, 若上式不成立, 则 h 不是 $\#E(\mathbb{F}_p)$; 若对随机挑选的几个 $P' \in E(\mathbb{F}_p)$ 都有 $hP' = \mathcal{O}$, 则可以认为 h 是 $\#E(\mathbb{F}_p)$ 的倍数, 当 h 为素数时, 就可以认为 $h = \#E(\mathbb{F}_p)$.

当 $hP = \mathcal{O}$ 时, 就有 $(p + 1 - c_3) \cdot P - r_1m_2m_3 \cdot P = r_2m_1m_3 \cdot P$.

§5.6 计算 $t \bmod l^n$

假设 $x^2 - tx + p \mod l$ 在 $\mathbb{F}_l$ 中有两个不同的根 τ_1 和 τ_2, 因而存在 $\mathbb{F}_p$ 上的两条曲线 E_1 和 E_2 及定义在 $\mathbb{F}_p$ 上的同种映射 (见推论 2.2)

$$I_i: \quad E \longrightarrow E_i$$

$$(x, y) \longmapsto \left(\frac{k_i(x)}{h_i^2(x)}, \frac{g_i(x, y)}{h_i^3(x)}\right),$$

其中, $\deg h_i(x) = (l-1)/2, \quad \deg k_i(x) = l, i = 1, 2$.

E 的 Tate 模 $T_l(E) = \varprojlim_n E[l^n]$(见 §3.4), $T_l(E)$ 中任一元素可表示为

$$(p_1, p_2, \cdots, p_n, \cdots) \in T_l(E): \quad p_n \in E[l^n], \ lp_n = p_{n-1},$$

$T_l(E)$ 中的加法定义为按分量相加

$$(p_1, p_2, \cdots, p_n, \cdots) + (q_1, q_2, \cdots, q_n, \cdots) = (p_1 + q_1, p_2 + q_2, \cdots),$$

$T_l(E)$ 是 $\mathbb{Z}_l$ 上的模, 这里 $\mathbb{Z}_l = \varprojlim_n \mathbb{Z}/l^n\mathbb{Z}$, $\mathbb{Z}_l$ 中任一元素表为

$$(\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots) \in \mathbb{Z}_l, \quad \alpha_n \in \mathbb{Z}/l^n\mathbb{Z}, \quad \alpha_n \mod l^{n-1} = \alpha_{n-1},$$

$\mathbb{Z}_l$ 在 $T_l(E)$ 上的作用定义为

$$(\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots) \cdot (p_1, p_2, \cdots, p_n, \cdots) = (\alpha_1 p_1, \alpha_2 p_2, \cdots, \alpha_n p_n, \cdots),$$

E 上 l^n 阶点的集合 $E[l^n] \cong \mathbb{Z}/l^n\mathbb{Z} \times \mathbb{Z}/l^n\mathbb{Z}$ 是 $\mathbb{Z}/l^n\mathbb{Z}$ 上秩为 2 的模, 同样 $T_l(E) \cong \mathbb{Z}_l \times \mathbb{Z}_l$ 是 $\mathbb{Z}_l$ 上秩为 2 的模 $(l \neq p)$.

E 上的 Frobenius 变换 ϕ 在 $T_l(E)$ 上产生一个 $\mathbb{Z}_l$ 变换

$$\phi(p_1, p_2, \cdots, p_n, \cdots) = \big(\phi(p_1), \phi(p_2), \cdots, \phi(p_n), \cdots\big),$$

因

$$\begin{aligned} l^n \cdot \phi(p_n) &= \phi\big(l^n(p_n)\big) = \mathcal{O} \Longrightarrow \phi(p_n) \in E[l^n] \quad (\phi\text{与}[l]\text{可交换}), \\ l \cdot \phi(p_n) &= \phi\big(l(p^n)\big) = \phi(p_{n-1}), \end{aligned}$$

同时也有

$$\begin{aligned} &\phi\big((\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots)(p_1, p_2, \cdots, p_n, \cdots,)\big) \\ =&(\alpha_1, \alpha_2, \cdots, \alpha_n, \cdots)\phi(p_1, p_2, \cdots, p_n, \cdots). \end{aligned}$$

ϕ 的特征多项式为 $x^2 - tx + p$, ϕ 可用 $\mathbb{Z}_l$ 上的一个矩阵表示.

当 $x^2 - tx + p$ 在 F_l 上有两个不同的根 τ_1 和 τ_2 时, 它在 $\mathbb{Z}_l$ 上也有两个不同的根, 仍记为 τ_1 和 τ_2, ϕ 在 $T_l(E)$ 上有两个不同的本征子空间 T_1^E 和 T_2^E, 分别对应本征值 τ_1 和 τ_2.

设 $I_i: \quad E \longrightarrow E_i$ 为定义在 $\mathbb{F}_p$ 上的同种映射, 它与 ϕ 是可交换的, $(\phi^2 - t\phi + p) \cdot T_l(E) = \mathcal{O}_E$. I_i 产生一个映上的映射 $T_l(E) \longrightarrow T_l(E_i)$,

$$\begin{aligned} (\phi^2 - t\phi + p) \cdot T_l(E_i) &= (\phi^2 - t\phi + p) I_i\big(T_l(E)\big) \\ &= I_i \cdot (\phi^2 - t\phi + p) \cdot T_l(E) \\ &= \mathcal{O}_{E_i}, \end{aligned}$$

所以 ϕ 在 $T_l(E_i)$ 上具有相同的特征多项式, 即有相同的特征根 τ_1, τ_2.

$T_l(E_i)$ 对应的两个本征子空间记为 $T_i^{E_j} \quad (j = 1, 2, i = 1, 2)$.

$E_1[l]$ 中也存在对应的两个本征子空间 $T_1^{E_1} \cap E_1[l]$, $T_2^{E_1} \cap E_1[l]$ ($T_i^{E_1} \cap E_1[l]$ 表示 $T_i^{E_1}$ 中第一坐标的集合), 因而也存在两个 $\mathbb{F}_p$ 上的曲线 E_{11} 和 E_{12} 与 E_1 在 $\mathbb{F}_p$ 上同种, $I_{1i}: E_1 \longrightarrow E_{1i}$.

同种映射 $I_1 : E \longrightarrow E_1$, 其核为 $T_1^E \cap E[l]$, 它的对偶 (见 §3.3)$\widehat{I}_1 : E_1 \longrightarrow E$ 的核一定是 $T_i^E \cap E_1[l]\,(i = 1, 2)$ 中的一个 (因为 $\widehat{I}_1 \cdot I_1 = [l], |\mathrm{Ker}\widehat{I}_1| = l$), 所以 $\widehat{I}_1$ 为 I_{11} 或 I_{12}. 易见 $I_1\big(T_1^E \cap E[l]\big) = \mathcal{O}_{E_1}$, $I_1(T_2^E \cap E[l])$ 是 $E_1[l]$ 中的 l 阶子群, 且是 ϕ

对应 τ_2 的如下本征子空间:

$$\phi\big(I_1(T_2^E\bigcap E[l])\big) = I_1\phi\big(T_2^E\bigcap E[l]\big) = I_1\cdot\tau_2\big(T_2^E\bigcap E[l]\big) = \tau_2\cdot I_1\big(T_2^E\bigcap E[l]\big),$$
$$\widehat{I}_1\big(I_1(T_2^E\bigcap E[l])\big) = l\big(T_2^E\bigcap E[l]\big) = \mathcal{O}_E,$$

所以 $I_1\big(T_2^E\cap E[l]\big)\subset \mathrm{Ker}\widehat{I}_1$, 可见 $\widehat{I}_1 = I_{1,2}$.

考虑

$$E \xrightarrow{I_1} E_1 \xrightarrow{I_{11}} E_{11}.$$

$\mathrm{Ker}(I_{11}\cdot I_1)$ 是 E 中一个 l^2 阶子群, 故 $\mathrm{Ker}(I_{11}\cdot I_1)$ 是 $E[l^2]$ 的一个子群, 可以通过计算 $I_{11}\cdot I_1$ 表达式得到 E 上的 l^2 阶除子多项式 $f_{l^2}^E(x)$ 的一个因子. 我们有

$$I_1(x,y) = \left(\frac{k_1(x)}{h_1(x)^2}, \frac{g(x,y)}{h_1(x)^3}\right).$$

由算法 5.3, 得到 E_1 的方程 $y^2 = x^3 + \widehat{a}x + \widehat{b}$, 由算法 5.4 得到 $h_1(x)$(即 $h(x)$), $\deg h_1(x) = (l-1)/2$.

通过

$$\wp_1(z) = \frac{k_1\big(\wp(x)\big)}{h_1\big(\wp(z)\big)^2}$$

可以得 $k_1(x)(\deg k_1(x) = l)$.

同样, 通过算法 5.3, 得 E_{11} 的方程

$$I_{11}(x,y) = \left(\frac{k_{11}(x)}{h_{11}(x)^2}, \frac{g_{11}(x,y)}{h_{11}(x)^3}\right).$$

由算法 5.4, 得 $h_{11}(x)$, 在 $I_{11}\cdot I_1$ 的分母中出现的因子

$$h_{11}\left(\frac{k_1(x)}{h_1(x)^2}\right)\cdot h_1(x)^{l-1}$$

为 $f_{l^2}^E(x)$ 的因子, 记之为 $g(x)$, 次数为 $l(l-1)/2$.

计算 λ $(0\leqslant\lambda<l)$, 使得

$$(x^q, y^q) = (\mu_1+\lambda l)(x,y) = \mu_1(x,y) + \lambda l(x,y) \pmod{E(x,y), g(x)}.$$

记 $\alpha_1 = \mu_1 + \lambda l \pmod{l^2}$, 则 $t\equiv \alpha_1 + p\alpha_1^{-1} \pmod{l^2}$.

设 E 的不变量为 j_0, $\Phi_l^c(X, j_0)$ 在 $\mathbb{F}_p$ 中有两个根 g_1 和 g_2, $\Phi_l^c(l^s/g_1, Y)$ 的根即为 E 的所有同种曲线的 j 不变量, 其中包括 j_0 及 j_1 (E_1 的不变量). $\Phi_l^c(X, j_1)$ 在 $\mathbb{F}_p$ 中也有两个根, 其中一个即为 l^s/g_1, 我们排除这一个, 而取另一个, 即取 $\Phi_l^c(X, j_1)/\big(X - w_l(g_1)\big)$ 的根.

类似地利用 n 层复合同种映射, 可以得到 $t \bmod l^n$.

§5.7 算法汇总

(算法 5.1) 计算模多项式 $\Phi_l^c(X,Y)$

输入: $f(\tau)$ 和 $j(l\tau)$ 的展开式至 q^{lv} 项.

输出: $a_{r,k}$, $0 \leqslant r \leqslant v$, $0 \leqslant k \leqslant v$.

Step 1. Set $a_{l+1,k} := 0$, $1 \leqslant k \leqslant v$; $a_{l+1,0} := 1$;

Step 2. Set $s_0(\tau) := 1$, $h_1(\tau) := 1$, $h_2(\tau) := 1$;

Step 3. for $r = 1, \cdots, l+1$

3.1 $h_1(\tau) := h_1(\tau) \cdot f(\tau)$ /* $h_1(\tau) = f(\tau)^r$ */;

3.2 利用 (5.12) 式由 $h_1(\tau)$ 计算 $c_{r,1}(\tau)$, 展开到 $q^{l\lfloor\frac{v(l+1-r)}{l}\rfloor}$;

3.3 $h_2(\tau) = h_2(\tau) \cdot l^s / f(l\tau)$;

3.4 $c_r(\tau) := c_{r,1}(\tau) + h_2(\tau)$ /* $h_2(\tau) = (l^s/f(l\tau))^r$ */;

3.5 利用 (5.11) 式计算 $s_r(\tau)$, 展开到 $q^{l\lfloor\frac{v(l+1-r)}{l}\rfloor}$;

3.6 for $k = v, v-1, \cdots, 0$

3.6.1 $a_{l+1-r,k} := (-1)^r s_r(\tau)$ 的 $q^{-l/k}$ 项系数;

3.6.2 $(-1)^r s_r(\tau) := (-1)^r s_r(\tau) - a_{l+1-r,k} j(l\tau)^k$;

3.7 If $s_r(\tau) = 0$, Then return $\{a_{r,0}, a_{r,1}, \cdots, a_{r,v}\}$.

(算法 5.2) 计算 $\Phi_l(X,j)$ 在 $\mathbb{F}_p$ 中的根

输入: j.

输出: g.

Step 1. 计算 $\gcd(x^p - x, \Phi_l(X,j))$

Step 2. 若 $\gcd \neq 1$

2.1 则计算 gcd 的根 g, 输出;

Step 3. 否则

3.1 l 为 Atkin 素数.

(算法 5.3)　计算同种椭圆曲线及 p_1(l 为 Elkies 素数)

输入: $(a,b)\in\mathbb{F}_p^2$, $\Phi_l^c(X,j)$ 的根 $g\in\mathbb{F}_p$, $s\in\mathbb{Z}$.

输出: $(E/\mathcal{C},p_1)=(\widehat{a},\widehat{b},p_1)$.

Step 1. 计算 $E_4:=-3^{-1}a$, $E_6:=-2^{-1}b$, $\Delta:=1728^{-1}(E_4^3-E_6^2)$, $\Delta^{(l)}:=l^{-12}\cdot\Delta\cdot g^{12/s}$, $j:=E_4^3/\Delta$;

Step 2. 计算

$$D_G:=g\cdot\Big(\frac{\partial}{\partial X}\Phi_l(X,Y)\Big)(g,j),\qquad D_J:=j\cdot\Big(\frac{\partial}{\partial Y}\Phi_l(X,Y)\Big)(g,j);$$

Step 3. 若 $D_J=0$

3.1 $E_4^{(l)}:=l^{-2}E_4$, $\quad\widehat{a}:=-3l^4E_4^{(l)}$, $\quad j^{(l)}:=(E_4^{(l)})^3\cdot(\Delta^{(l)})^{-1}$;

3.2 输出 $\{\widehat{a},\pm2l^6\sqrt{(j^{(l)}-1728)\cdot\Delta^{(l)}},0\}$;

Step 4. 否则

4.1 计算 $E_2^*:=-(12/s)E_6\cdot DJ\cdot(E_4\cdot DG)^{-1}$;

4.2 计算 $E_0:=E_6\cdot(E_4\cdot E_2^*)^{-1}$;

4.3 计算 $g':=-(s/12)E_2^*g$ 及 $j':=-E_4^2\cdot E_6\cdot\Delta^{-1}$;

4.4 计算 D_G', D_J'

$$D_G':=g'\Big(\frac{\mathrm{d}\Phi_l(X,Y)}{\mathrm{d}X}\Big)(g,j)+g\Big[g'\Big(\frac{\mathrm{d}^2\Phi_l(X,Y)}{\mathrm{d}X^2}\Big)(g,j)+j'\Big(\frac{\mathrm{d}^2\Phi_l(X,Y)}{\mathrm{d}X\mathrm{d}Y}\Big)(g,j)\Big];$$

$$D_J':=j'\Big(\frac{\mathrm{d}\Phi_l(X,Y)}{\mathrm{d}Y}\Big)(g,j)+j\Big[j'\Big(\frac{\mathrm{d}\Phi_l(X,Y)}{\mathrm{d}Y^2}\Big)(g,j)+g'\Big(\frac{\mathrm{d}^2\Phi_l(X,Y)}{\mathrm{d}X\mathrm{d}Y}\Big)(g,j)\Big];$$

4.5 计算 $E_0':=\big((-s/12)D_G'-E_0D_J'\big)(DJ)^{-1}$

4.6 计算 $E_4^{(l)}:=l^{-2}\big(E_4-E_2^*[12E_0'\cdot E_0^{-1}+6E_4^2\cdot E_6^{-1}-4E_6E_4^{-1}]+(E_2^*)^2\big)$;

4.7 计算 $j^{(l)}:=\big(E_4^{(l)}\big)^3\cdot\big(\Delta^{(l)}\big)^{-1}$;

4.8 计算 $f:=l^s\cdot g^{-1}$ 及 $f':=(s/12)E_2^*f$;

4.9 计算

$$DG_2:=\Big(\frac{\mathrm{d}}{\mathrm{d}X}\Phi_l(X,Y)\Big)(f,j^{(l)}),\qquad DJ_2:=\Big(\frac{\mathrm{d}}{\mathrm{d}Y}\Phi_l(X,Y)\Big)(f,j^{(l)});$$

4.10 计算 $j^{(l)\prime}:=-l^{-1}\cdot f'DG_2\cdot DJ_2^{-1}$;

4.11 计算 $E_6^{(l)}:=-E_4^{(l)}\cdot j^{(l)\prime}\big(j^{(l)}\big)^{-1}$;

Step 5. 置

$$\widehat{a}:=-3l^4E_4^{(l)},\quad\widehat{b}:=-2l^6E_6^{(l)},\quad p_1:=-2^{-1}lE_2^*;$$

Step 6. 输出 $\{(\widehat{a},\widehat{b},p_1)\}$.

(算法 5.4) 计算除子多项式的因子 $h(x)$

输入：椭圆曲线 (a,b) 及 $(\widehat{a},\widehat{b},p_1)$.

输出：$h(x)=x^d+a_{d-1}x^{d-1}+\cdots+a_0$.

Step 1. For $n=0$ to l

1.1 计算 $\psi_n(x,y)$, ($n=0,1,2,3,4$ 直接输入)

$$\psi_{2m+1}=\psi_{m+2}\psi_m^3-\psi_{m+1}^3\psi_{m-1}, \qquad m\geqslant 2;$$
$$\psi_{2m}=\psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m+1}^2\psi_{m-2})/2y, \qquad m\geqslant 3;$$

Step 2. Set $d:=(l-1)/2,\ \ a_d:=1$;

Step 3. For $k=1,2,\cdots,(l-3)/2$;

3.1 利用 a,b 计算 c_k /* $\left(\wp=\frac{1}{z^2}+\sum\limits_{k=1}^{\infty}c_kz^{2k}\right)$ */;

Step 4. Set $w\wp_1(z):=\frac{1}{z^2}+\sum\limits_{k=1}^{(l-3)/2}c_kz^{2k}$ /* $\wp(z)$ 展开至 $l-3$ 次项 */;

Step 5. For $j=2,3,\cdots,d$

5.1 计算 $w\wp_j(z):=w\wp_{j-1}(z)\cdot w\wp_1(z)$ /* $\wp(z)^j$ 展开至 $l-3$ 次项 */;

Step 6. For $k=1,\cdots,(l-3)/2$

6.1 利用 $\widehat{a},\widehat{b}$, 计算 $\widehat{c}_k$;

Step 7. Set

$$g(z):=z^{1-l}\sum_{r=0}^{(l-1)/2}(r!)^{-1}\left(\sum_{k=1}^{(l-3)/2}(lc_k-\widehat{c}_k)\cdot\big((2k+1)(2k+2)\big)^{-1}z^{2k+2}-p_1z^2\right)^r;$$

Step 8. For $j=d-1,\cdots,0$

8.1 Set $g(z):=g(z)-a_{j+1}w\wp_{j+1}(z)$;

8.2 计算 $a_j:=g(z)$ 的最低次项系数 /* 可能为零 */;

Step 9. Set $h(x):=x^d+a_{d-1}x^{d-1}+\cdots+a_1x+a_0$;

Step 10. If $h(x)|\psi_l(x)$, Then 输出 $h(x)$.

(算法 5.5) 计算 t mod l

输入：$E=(a,b),\ \ h(x)\in\mathbb{F}_p[x]$.

输出：t mod l.

Step 1. For $n=0$ to $(l+3)/2$

1.1 计算 $\psi_n(x,y)$,　$(n=0,1,2,3,4$ 直接输入)

$$\psi_{2m+1}=\psi_{m+2}\psi_m^3-\psi_{m+1}^3\psi_{m-1},\qquad m\geqslant 2$$
$$\psi_{2m}=\psi_m(\psi_{m+2}\psi_{m-1}^2-\psi_{m+1}^2\psi_{m-2})/2y,\qquad m\geqslant 3;$$

Step 2. 计算

$$l_x:=x^p \pmod{h(x)},\qquad l_y:=y(x^3+ax+b)^{(p-1)/2} \pmod{h(x)};$$

Step 3. For $\alpha=1$ to $(l-1)/2$
  3.1 $r_x:=x\psi_\alpha^2-\psi_{\alpha-1}\cdot\psi_{\alpha+1} \pmod{h(x)}$;
  3.2 If $l_x\cdot\psi_\alpha^2\equiv r_x \pmod{h(x)}$;
    3.2.1 $r_y:=\psi_{\alpha+2}\psi_{\alpha-1}^2-\psi_{\alpha-2}\psi_{\alpha+1}^2 \pmod{h(x)}$;
    3.2.2 If $4yl_y\cdot\psi_\alpha^3\equiv r_y \pmod{h(x)}$;
      3.2.2.1 Return　$t\equiv\alpha+p\alpha^{-1} \pmod{l}$;
    3.2.3 If　$4yl_y\psi_\alpha^3\equiv -r_y \pmod{h(x)}$;
      3.2.3.1 Return　$t\equiv-\alpha-p\alpha^{-1} \pmod{l}$.

(算法 5.6)　Atkin 算法

输入：曲线 E 的不变量 j $(\neq 0,1728)$, $l(<p)$, $\Phi_l^c(x,y)$.
输出：$t \bmod l$ 的值.
Step 1. Set $\widetilde{\Phi}(x):=\Phi_l^c(x,j)$;
Step 2. 计算 $d_1:=\deg\left(\gcd(x^p-x,\widetilde{\Phi}(x))\right)$;
Step 3. If $d_1\geqslant 1$
  3.1 算法 2, 算法 3, 算法 4, 算法 5;
  3.2 If 算法 5 没有输出, then goto 4;
  3.3 else return;
Step 4. If $d_1=1$　　/⋆　$(1,l)$ 型　⋆/
  4.1 Then Return $\{\pm 2\sqrt{p} \pmod{l}\}$;
Step 5. If $d_1=l+1$　　/⋆　$(1,1,\cdots,1)$ 型　⋆/
  5.1 Then set $\alpha:=\sqrt{p} \pmod{l}$;
  5.2 Return $\{\pm(\alpha+p\alpha^{-1}) \pmod{l^2}\}$;
Step 6. Set $\widetilde{G}(x):=\widetilde{\Phi}(x)/\gcd(x^p-x,\Phi_l(x,j))$;
Step 7. Set $d_{\text{rest}}:=\deg\widetilde{G}(x)$;

Step 8. If $\left(\frac{p}{l}\right)=1$

8.1 For all d : $d|d_{\text{rest}}$, $\frac{d_{\text{rest}}}{d}$ 是偶数;

8.1.1 计算 $d_2 := \deg(\gcd(x^{p^d}-x, \widetilde{G}(x)))$;

8.1.2 If $d_2>0$, $d_1=2$ /⋆ $(1,1,d,d,\cdots,d)$型 ⋆/;

8.1.2.1 Return $\left\{(\zeta_d+1)\cdot\sqrt{p\zeta_d^{-1}};\ \zeta_d\in\mathbb{F}_l,\ \mathrm{ord}(\zeta_d)=d\right\}$;

8.1.3 If $d_2>0$, $d_1=0$ /⋆ $(d,d,\cdots,d)$型 ⋆/;

8.1.3.1 Return $\left\{(\zeta_d+1)\cdot\sqrt{p\zeta_d^{-1}};\ \zeta_d\in\mathbb{F}_{l^2},\ \mathrm{ord}(\zeta_d)=d\right\}$;

Step 9. Else

9.1 For all d : $d|d_{\text{rest}}$, $\frac{d_{\text{rest}}}{d}$ 是奇数;

9.1.1 计算 $d_2 := \deg(\gcd(x^{p^d}-x, \widetilde{G}(x)))$;

9.1.2 If $d_2>0$, $d_1=2$ /⋆ $(1,1,d,d,\cdots,d)$型 ⋆/;

9.1.2.1 Return $\left\{\pm(\zeta_d+1)\cdot\sqrt{p\zeta_d^{-1}};\ \zeta_d\in\mathbb{F}_l,\ \mathrm{ord}(\zeta_d)=d\right\}$;

9.1.3 If $d_2>0$, $d_1=0$ /⋆ $(d,d,\cdots,d)$型 ⋆/

9.1.3.1 Return $\left\{\pm(\zeta_d+1)\cdot\sqrt{p\zeta_d^{-1}};\ \zeta_d\in\mathbb{F}_{l^2},\ \mathrm{ord}(\zeta_d)=d\right\}$.

(算法 5.7)　　信息的综合

输入: $\mathcal{C}_1$, $\mathcal{C}_2$, c_3, m_1, m_2, m_3.

输出: 阶 h.

Step 1. 任取一点 $P\in E(\mathbb{F}_q)$, Set

$$Q_0:=(q+1-c_3)P,\qquad Q_1:=(m_2m_3)\cdot P,\qquad Q_2:=(m_1m_3)\cdot P,$$
$$Q_3:=(m_1m_2m_3)\cdot P,\qquad h:=0;$$

Step 2. For all $x\in\mathcal{C}_1$

2.1 Set $r_1'\equiv(x-c_3)(m_2m_3)^{-1} \mod m_1$, $\left\lfloor\frac{-m_1}{2}\right\rfloor<r_1'\leqslant\left\lfloor\frac{m_1}{2}\right\rfloor$;

2.2 计算 $H:=Q_0-r_1'Q_1$, 制表 (H,r_1');

Step 3. For all $y\in\mathcal{C}_2$

3.1 Set $r_2'\equiv(y-c_3)(m_1m_3)^{-1} \mod m_2$, $-m_2\leqslant r_2'<0$;

3.2 If $r_2'=-m_2$, $(-Q_3,r_2')$ 在表中出现;

3.2.1 Set $h:=q+1-c_3-r'm_2m_3+m_1m_2m_3$;

Step 4. 计算 $H_1:=r_2'Q_2$, $H_2:=r_2'Q_2+Q_3$;

Step 5. If (H_1, r') 在表中出现

5.1 Then $h := q + 1 - c_3 - r'm_2m_3 - r_2'm_1m_3$;

Step 6. If (H_2, r') 在表中出现

6.1 Then $h := q + 1 - c_3 - r'm_2m_3 - (r_2' + m_2)m_1m_3$;

Step 7. If 另取几个 $P' \in E(F_1)$, 都有 $h \cdot P' = \mathcal{O}$;

7.1 Then Return h.

(算法 5.8) 计算 $t \mod l^n$

输入: E, p, l, n.

输出: $t \mod l^n$.

Step 1. 找出 $\Phi_l(X, j(E))$ 在 $\mathbb{F}_q$ 中的根;

Step 2. 如果 $\Phi_l(X, j(E))$ 在 $\mathbb{F}_q$ 中有两个不同的根

2.1 由算法 3, 算法 4 计算 E_1 的方程 $\mathcal{E}_1(x, y)$ 及 $h_1(x)$;

2.2 找本征值 $\tau_1 (= \alpha)$;

2.3 For $k = 2$ to n

2.3.1 找出 $\Phi_l^c(X, j(E_{k-1}))/(X - w_l(\tau_1))$ 在 $\mathbb{F}_p$ 的根, 计算 E_k 的方程 $\mathcal{E}_k$;

2.3.2 计算 I_k : $E_{k-1} \longrightarrow E_k$ 及 $f_l^{E_{k-1}}$ 的因子 h_k;

2.3.3 由 $h_k \circ I_{k-1} \circ \cdots \circ I_2 \circ I_1$, 计算 $f_{l^k}^E$ 的因子 g, 阶为 $l^{k-1}(l-1)/2$;

2.3.4 找 λ $(0 \leqslant \lambda < l)$, 求 $\tau_k = \tau_{k-1} + \lambda l^{k-1}$, 使得

$$(x^p, y^p) = \tau_{k-1}(x, y) + \lambda\big(l^{k-1}(x, y)\big) \mod \big(\mathcal{E}, g(x)\big);$$

2.4 输出 $\tau_n + p\tau_n^{-1} \pmod{l^n}$.

第三部分

提升到局部域上的点数计算算法

第六章 p-adic 数

§6.1 p-adic 数的引入

我们考虑解下述同余方程：

$$f(x) \equiv 0 \pmod{p^l}, \tag{6.1}$$

此处 $f(x)$ 为一整系数多项式, p 为一素数, 为此先解同余式

$$f(x) \equiv 0 \pmod{p}, \tag{6.2}$$

若 (6.2) 式有解 a_0, $0 \leqslant a_0 < p$, 且 $f'(a_0) \not\equiv 0 \pmod{p}$, 则命 $x = a_0 + py$ 并讨论同余式

$$f(a_0 + py) \equiv 0 \pmod{p^2}, \qquad 0 \leqslant y < p,$$

即

$$f(a_0)/p + f'(a_0)y \equiv 0 \pmod{p}, \qquad 0 \leqslant y < p,$$

由此式惟一地定出 y, 令之为 a_1, 如果

$$x = a_0 + a_1 p, \qquad 0 \leqslant a_0, a_1 < p,$$

则是 $f(x) \equiv 0 \pmod{p^2}$ 之一解.

一般地, 若

$$x = x_0 = a_0 + a_1 p + a_2 p^2 + \cdots + a_{l-2} p^{l-2},$$
$$0 \leqslant a_v < p, v = 0, 1, \cdots, l-2$$

是同余式

$$f(x) \equiv 0 \pmod{p^{l-1}}$$

之一解, 且 $f'(x_0) \not\equiv 0 \pmod{p}$, 则令 $x = x_0 + p^{l-1}y$, 并研究

$$f(x_0 + p^{l-1}y) \equiv 0 \pmod{p^l}, \qquad 0 \leqslant y < p,$$

即

$$f(x_0)/p^{l-1} + f'(x_0)y \equiv 0 \pmod p, \qquad 0 \leqslant y < p,$$

因此定出惟一的 y, 令其为 a_{l-1}, 则

$$x = a_0 + a_1 p + \cdots + a_{l-1}p^{l-1}, \quad 0 \leqslant a_v < p, \ v = 0, 1, \cdots, l-1$$

乃是方程 (6.1) 的解.

如果这种手续可以无穷下去, 则形式上我们得出一个关于 p 的幂级数

$$a_0 + a_1 p + \cdots a_l p^l + \cdots, \qquad 0 \leqslant a_v < p, \tag{6.3}$$

这个幂级数称为方程式 $f(x) = 0$ 的一个 p-adic 解.

我们知道, 在用逐步接近法解 $f(x) = 0$ 的实数解时, 若进行的次数越多, 亦即小数点后所取位数越多, 则所得解就越精确, 在此, 利用逐次解同余式

$$f(x) \equiv 0 \pmod p, \qquad f(x) \equiv 0 \pmod{p^2}, \cdots, f(x) \equiv 0 \pmod{p^l},$$

以求 $f(x) = 0$ 的 p-adic 解时, 也有类似情形, 亦即取 l 越大, 则最后的同余式的解

$$x = a_0 + a_1 p + \cdots + a_{l-1}p^{l-1}, \quad 0 \leqslant a_v < p$$

越接近 $f(x) = 0$ 的 p-adic 解.

称形如 (6.3) 式的 p 的幂级数为一个 p-adic 数, 但这不是 p-adic 数的全部. 一般而言, p-adic 数可以有有限个 p 的负幂, 即 p-adic 数的一般形式为

$$a_{-n}p^{-n} + \cdots + a_0 + a_1 p + \cdots + a_l p^l + \cdots, \qquad 0 \leqslant a_v < p, \tag{6.4}$$

这与每一个实数可表为 10 进制位无穷小数

$$a_{-n}10^n + \cdots + a_0 + a_1 10^{-1} + \cdots + a_l 10^{-l} + \cdots, \qquad 0 \leqslant a_v < 10$$

类似.

2 个 p-adic 数

$$a_{-n}p^{-n} + \cdots + a_0 + a_1 p + \cdots + a_l p^l + \cdots, \qquad 0 \leqslant a_v < p,$$

$$b_{-m}p^{-m} + \cdots + b_0 + b_1 p + \cdots + b_l p^l + \cdots, \qquad 0 \leqslant b_v < p$$

之和及差 (设 $n \geqslant m$), 即为对应项系数相加及相减所得:

$$a_{-n}p^{-n} + \cdots + a_{-m-1}p^{-m-1} + (a_{-m} \pm b_{-m})p^{-m} + \cdots$$
$$+ (a_0 \pm b_0) + (a_1 \pm b_1)p + \cdots + (a_l \pm b_l)p^l + \cdots .$$

但若相加后所得的系数有不小于 p 者, 则应向后进一位, 例如 $a_v + b_v \geqslant p$, 则命 $(a_v + b_v)p^v = (a_v + b_v - p)p^v + p^{v+1}$, 再把 p^{v+1} 加到后一项中去. 同样, 若相减后系数有小于 0 者, 则应向后借一位, 例如 $a_v - b_b < 0$, 则令

$$(a_v - b_v)p^v + (a_{v+1} - v_{v+1})p^{v+1} + \cdots \text{ 为 } (a_v - b_v + p)p^v$$
$$+ (a_{v+1} - b_{v+1} - 1)p^{v+1} + \cdots .$$

总之, 最后使得所有系数皆为小于 p 的非负整数.

类似可进行两个 p-adic 数之积, 两个 p-adic 数之积同于通常幂级数的乘积, 而所得的结果中也应将不小于 p 的系数向后进位, 直至所有系数皆为小于 p 的非负整数.

例 6.1 方程 $3x = 2$ 的 5-adic 解是

$$4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots ,$$

式中除了第一项外, 其余各项系数轮流为 1 和 3 两数.

证明 要证明这点, 可利用解同余式的方法进行, 但也可由直接验算得知

$$\begin{aligned}
&3 \cdot (4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + \cdots) \\
&= 12 + 3 \cdot 5 + 9 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \cdots \\
&= 2 + (2 + 3) \cdot 5 + 9 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \cdots \\
&= 2 + 10 \cdot 5^2 + 3 \cdot 5^3 + 9 \cdot 5^4 + \cdots \\
&= 2 + 5 \cdot 5^3 + 9 \cdot 5^4 + \cdots = 2 + 10 \cdot 5^4 + \cdots \\
&= 2.
\end{aligned}$$

例 6.2 方程 $x^2 = 7$ 的一个 3-adic 解是 $1 + 1 \cdot 3 + 1 \cdot 3^2 + 0 \cdot 3^3 + 2 \cdot 3^4 + \cdots$.

设 a 为一有理数, 则方程 $x = a$ 的 p-adic 解称为 a 的 p-adic 表示法. 现设 d 为正整数, 则 $x = d$ 的 p-adic 解即: $d_0 + d_1 p + \cdots + d_l p^l$($d$ 的 p 进制表示).

§6.2 赋 值

在 §6.1 中, 我们是形式地讨论, 并没有涉及幂级数

$$a_{-n}p^{-n} + \cdots + a_0 + a_1 p + \cdots + a_l p^l + \cdots \qquad 0 \leqslant a_v < p$$

的收敛性, 但显然该级数在通常意义下是不收敛的. 现在引进赋值的概念, 它是通常实数的绝对值概念的抽象和推广, 且有与绝对值类似的性质.

定义 6.1　设 $\Phi:\mathbb{Q}\to\mathbb{R}$ 为一函数, 满足

(1) $\Phi(a)\geqslant 0,\quad \Phi(a)=0 \iff a=0$;

(2) $\Phi(ab)=\Phi(a)\Phi(b)$;

(3) $\Phi(a+b)\leqslant\Phi(a)+\Phi(b)$.

则称 Φ 为 $\mathbb{Q}$ 上的一个赋值.

显然, 我们有

性质 6.2　(1) $\Phi(1)=\Phi(-1)=1$;

(2) $\Phi(a)=\Phi(-a)$;

(3) $\Phi(n)\leqslant n,\quad \forall n\in\mathbb{N}$;

(4) $\Phi(a+b)\geqslant\Phi(a)-\Phi(b),\quad \Phi(a+b)\geqslant\Phi(b)-\Phi(a)$.

例 6.3

(1) $\Phi(a)=1,\quad \forall a\neq 0, \Phi(0)=0$ 为一平凡赋值, 记为 Φ_0;

(2) $\Phi(a)=|a|$, 为一赋值;

(3) 令 p 为一固定的素数, 则任一不等于 0 的有理数 a 可以惟一表为

$$a=p^n\cdot(r/s),\qquad s>0,$$

此处 r 和 s 为整数, $(r,s)=1$, $p\nmid rs$, n 为整数, 定义

$$\Phi(a)=\begin{cases}p^{-n}, & a\neq 0,\\ 0, & a=0,\end{cases}$$

则 Φ 为一赋值, 称之为 p-adic 赋值, 记为 $\Phi(a)=|a|_p$.

证明　(1) 和 (2) 显然; 今证 (3) 为赋值. 由定义显然赋值的前两条性质满足. 今设

$$a=\frac{r_1}{s_1}p^m,\qquad b=\frac{r_2}{s_2}p^n\quad (s_i>0,(r_i,s_i)=1,p\nmid r_is_i),$$

则

$$a+b=\frac{r_1s_2+r_2s_1p^{n-m}}{s_1s_2}p^m\quad (\text{不妨设}m\leqslant n).$$

由于 $p\nmid s_1s_2$, 故

$$|a+b|_p\leqslant p^{-m}=|a|_p\Longrightarrow |a+b|_p\leqslant|a|_p\leqslant|a|_p+|b|_p.$$

注 6.1 事实上, 由上面知

$$|a+b|_p \leqslant \max(|a|_p, |b|_p),$$

可进一步证明：若 $|a|_p \neq |b|_p$, 则

$$|a+b|_p = \max(|a|_p, |b|_p).$$

定义 6.3 设 Φ 与 Φ' 为两个赋值, 若有

$$\Phi(a) < \Phi(b) \iff \Phi'(a) < \Phi'(b),$$

则称 Φ 与 Φ' 等价.

例 6.4 设 Φ 为一赋值, $0 < s \leqslant 1$, 令 $\Phi' = \Phi^s$, 则易证 Φ' 亦为一赋值, 且 Φ' 与 Φ 等价.

定理 6.1 设 Φ 为一非平凡赋值, Φ' 与 Φ 等价, 则 $\Phi' = \Phi^s$ 对某个 $s > 0$.

证明 因为 $\Phi \neq \Phi_0$, 所以存在 a_0, 使得 $0 \leqslant \Phi(a_0) < 1$ (若 $\Phi(a_0) > 1$, 则 $\Phi(a_0^{-1}) < 1$). 对于任意有理数 $a \neq 0$, 有：对任意正整数 m, n, 下述成立：

$$\begin{aligned} \frac{m}{n} > \frac{\log \Phi(a)}{\log \Phi(a_0)} &\iff \Phi(a_0^m) < \Phi(a^n), \\ \frac{m}{n} > \frac{\log \Phi'(a)}{\log \Phi'(a_0)} &\iff \Phi'(a_0^m) < \Phi'(a^n), \end{aligned} \tag{6.5}$$

可见 $\frac{\log \Phi(a)}{\log \Phi(a_0)}$ 与 $\frac{\log \Phi'(a)}{\log \Phi'(a_0)}$ 均为适合 (6.5) 式的有理数 $\frac{m}{n}$ 的下极限, 从而

$$\frac{\log \Phi(a)}{\log \Phi(a_0)} = \frac{\log \Phi'(a)}{\log \Phi'(a_0)} \iff \frac{\log \Phi'(a)}{\log \Phi(a)} = \frac{\log \Phi'(a_0)}{\log \Phi(a_0)} = s > 0,$$

即 $\Phi'(a) = \Phi^s(a)$ $(s > 0)$, $\quad \forall a \in \mathbb{Q}$, 证毕.

定义 6.4 若存在一正整数 $n_0(>1)$, 使得 $\Phi(n_0) > 1$, 则称 Φ 为阿基米德赋值, 否则称 Φ 为非阿氏赋值.

例 6.5 $\Phi(a) = |a|$ 为阿氏的, Φ_0 及 $\Phi(a) = |a|_p$ 为非阿氏的.

定理 6.2 任一阿氏赋值等价于绝对值.

证明 设 Φ 为一阿氏赋值, $\forall n, n' \in \mathbb{N}$, 令

$$n' = a_0 + a_1 n + \cdots + a_v n^v, \qquad 0 \leqslant a_i < n, \quad a_v \neq 0,$$

则

$$\begin{aligned} \Phi(n') &\leqslant \Phi(a_0) + \Phi(a_1)\Phi(n) + \cdots + \Phi(a_v)\Phi(n^v) \qquad (\because \Phi(a_i) \leqslant a_i < n) \\ &\leqslant n(1 + \Phi(n) + \Phi(n)^2 + \cdots + \Phi(n)^v) \leqslant n(1+v)\max(1, \Phi(n)^v) \\ &\leqslant n\left(1 + \frac{\log n'}{\log n}\right)\max(1, \Phi(n)^{\log n'/\log n}). \end{aligned}$$

用 n'^h 代替 n', 得

$$\Phi(n') \leqslant \left(n\left(1+h\frac{\log n'}{\log n}\right)\right)^{1/h} \max\left(1, \Phi(n)^{\log n'/\log n}\right),$$

令 $h \to \infty$, 得

$$\Phi(n') \leqslant \max\left(1, \Phi(n)^{\log n'/\log n}\right), \quad \forall n, n' \in \mathbb{N}, \tag{6.6}$$

又 Φ 是阿氏的, 故存在 $n_0 > 1$, 使得 $\Phi(n_0) > 1$, 从而

$$1 < \Phi(n_0) \leqslant \max\left(1, \Phi(n)^{\log n_0/\log n}\right),$$

故对任意的 n 有

$$\Phi(n)^{\log n_0/\log n} > 1 \Longrightarrow \Phi(n) > 1,$$

而不等式 (6.6) 为

$$\Phi(n') \leqslant \Phi(n)^{\log n'/\log n} \Longrightarrow \frac{\log \Phi(n')}{\log n'} \leqslant \frac{\log \Phi(n)}{\log n}.$$

由 n 与 n' 的对称性, 知

$$\frac{\log \Phi(n')}{\log n'} = \frac{\log \Phi(n)}{\log n},$$

这说明存在 $s > 0$ 为正常数, 使得 $\frac{\log \Phi(n)}{\log n} = s > 0$, 即

$$\Phi(n) = n^s, \quad \forall n > 1.$$

由 $\Phi(n) \leqslant n \Longrightarrow s \leqslant 1$, 但 $\Phi(n) = \Phi(-n) \Longrightarrow \Phi(n) = |n|^s, \quad \forall n \in \mathbb{Z}$, 从而对一切 $a \in \mathbb{Q}$, 有

$$\Phi(a) = |a|^s, \qquad 0 < s \leqslant 1.$$

证毕.

定理 6.3　设 Φ 为一非阿赋值, 则

$$\Phi(a+b) \leqslant \max\left(\Phi(a), \Phi(b)\right).$$

如果 $\Phi(a) \neq \Phi(b)$, 则等号成立, 反之若赋值 Φ 适合上式, 则 Φ 为非阿氏的.

证明　由

$$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + b^n$$

知

$$\Phi\big((a+b)^n\big) \leqslant \Phi(a)^n + \Phi(a)^{n-1}\Phi(b) + \cdots + \Phi(a)\Phi(b)^{n-1} + \Phi(b)^n$$
$$\leqslant (n+1)\max\big(\Phi(a)^n, \Phi(b)^n\big),$$

即 $\Phi(a+b) \leqslant (n+1)^{1/n}\max(\Phi(a),\Phi(b))$, 令 $n\to\infty$ 得

$$\Phi(a+b) \leqslant \max(\Phi(a),\Phi(b)).$$

若 $\Phi(a)\neq\Phi(b)$, 设 $\Phi(a)>\Phi(b)$, 则由上可知 $\Phi(a+b)\leqslant\Phi(a)$, 若 $\Phi(a+b)<\Phi(a)$, 则

$$\Phi(a) = \Phi\big((a+b)-b\big) \leqslant \max\big(\Phi(a+b),\Phi(b)\big) < \Phi(a),$$

矛盾, 故

$$\Phi(a+b) = \Phi(a) = \max(\Phi(a),\Phi(b)).$$

反之, 若 Φ 适合 $\Phi(a+b)\leqslant\max(\Phi(a),\Phi(b))$, 则 $\forall n\in\mathbb{N}$, 有

$$\Phi(n) = \Phi(1+1+\cdots+1) \leqslant \max\Phi(1) = \Phi(1) = 1,$$

即 Φ 为非阿氏的, 证毕.

推论 6.1 若 Φ 为非阿赋值, 则对任意 $s>0$, Φ^s 均为一赋值 (不必假设 $s\leqslant 1$).

证明 Φ^s 显然满足赋值定义中前两条, 对于第 3 条, 有

$$\Phi^s(a+b) \leqslant \big(\max(\Phi(a),\Phi(b))\big)^s = \max(\Phi^s(a),\Phi^s(b)) \leqslant \Phi^s(a)+\Phi^s(b).$$

证毕.

对非阿赋值 Φ, 令 $w(a) = -\log\Phi(a)$, 则

(i) $\forall a\neq 0$, $w(a)$ 为实数, $w(0)=\infty$;

(ii) $w(ab) = w(a)+w(b)$;

(iii) $w(a+b)\geqslant\min(w(a),w(b))$, 若 $w(a)\neq w(b)$, 等号成立.

若 Φ 非平凡, 则存在 $a_0\in\mathbb{Q}$, 使得 $0<w(a_0)<\infty$. 由 Φ 的性质, 还可知

$$w(-a)=w(a),\quad w(1)=0,\quad w(n)\geqslant 0, \forall n\in\mathbb{Z}.$$

定理 6.4 二非平凡非阿赋值 Φ 与 Φ' 等价 $\Longleftrightarrow$ 存在 $s>0$, 使得 $w'(a) = sw(a), \forall a\in\mathbb{Q}$, 其中 $w'(a) = -\log\Phi'(a), w(a) = -\log\Phi(a)$.

证明 显然.

定理 6.5 任一非平凡的非阿赋值 Φ 均等价于某一个 p-adic 赋值 $|a|_p$.

证明　因 $\Phi \neq \Phi_0$, 故存在 $m \neq 1, m \in \mathbb{Z}$, 使得 $w(m) > 0$, 令

$$I = \{m \in \mathbb{Z} | w(m) > 0\}.$$

易知 I 为 $\mathbb{Z}$ 的一个理想, 从而 $I = \langle g \rangle, g \in \mathbb{N}$, 易验证 g 必为素数 (若 $g = g'g''$, $g' > 1, g'' > 1 \Longrightarrow w(g) = w(g') + w(g'')$, 但 $w(g) > 0, w(g') \geqslant 0, w(g'') \geqslant 0$, 故必有 $w(g') > 0$ 或 $w(g'') > 0 \quad \Longrightarrow g' \in I$ 或 $g'' \in I$, 这与 g 的定义矛盾). 令 $g = p$, 从而

$$w(n) = 0, \quad 若\ p \nmid n; \qquad w(n) > 0, \quad 若\ p | n.$$

对任一不为 0 的 $a \in \mathbb{Q}$, 令

$$a = \frac{r}{s} p^l, \quad s > 0, \quad (r, s) = 1, r, s, \in \mathbb{Z}, p \nmid rs,$$

则

$$w(a) = w\left(\frac{r}{s}\right) + w(p^l) = w(r) - w(s) + lw(p) = lw(p).$$

令 $w'(a) = -\log |a|_p = l \log p$, 则

$$w(a) = \frac{w(p)}{\log p} w'(a) = sw'(a), \qquad s = \frac{w(p)}{\log p} > 0,$$

于是由定理 6.4 知 Φ 与 $|a|_p$ 等价.

§6.3 完 备 化

定义 6.5　设 $(\mathbb{Q}, \varphi)$ 是 $\mathbb{Q}$ 上的一个赋值, 称 $\mathbb{Q}$ 中序列 $\{a_n\}_{n=1}^{\infty}$ 是关于 φ 的一个柯西序列, 是指 $\forall \varepsilon > 0$, 存在 N, 使得当 $m, n > N$ 时, 有 $\varphi(a_m - a_n) < \varepsilon$. 而 $\mathbb{Q}$ 中序列 $\{a_n\}_{n=1}^{\infty}$ (关于 φ) 收敛于 $a \in \mathbb{Q}$, 是指对每个 $\varepsilon > 0$, 均存在 N, 使得当 $m > N$ 时, $\varphi(a_m - a) < \varepsilon$.

注 6.2　所有关于赋值的概念, 均可在一般的域 F 上定义, 而不必限定在 $\mathbb{Q}$ 上.

定义 6.6　若 (F, φ) 是一个赋值域, 且 F 中每个柯西序列均收敛于 F 中某个元素, 则称 (F, φ) 是完备赋值域.

定理 6.6　设 $(\mathbb{Q}, \varphi)$ 是赋值域, 则一定存在一个赋值域 $(\widehat{F}, \widehat{\varphi})$, 使得

(1) $(\widehat{F}, \widehat{\varphi})$ 是完备赋值域;

(2) $\mathbb{Q}$ 在 $\widehat{F}$ 中是稠密的.

证明　令 $\widehat{F}$ 是 $\mathbb{Q}$ 上所有关于 φ 的柯西序列的全体模去下述等价关系 $\sim$:

$$\{a_n\} \sim \{b_n\} \iff \varphi(a_n - b_n) \to 0 \quad (n \to \infty\ 时),$$

即 $\widehat{F}=\{\overline{\{a_n\}}|\{a_n\}是柯西序列\}$.

在 $\widehat{F}$ 上定义加、减、乘、除如下：

$$\overline{\{a_n\}}\pm\overline{\{b_n\}}=\overline{\{a_n\pm b_n\}},\qquad \overline{\{a_n\}}\cdot\overline{\{b_n\}}=\overline{\{a_nb_n\}},$$

当 $\overline{\{b_n\}}$ 不等于 $\overline{\{0\}}$ 时, 定义

$$\overline{\{a_n\}}\cdot\overline{\{b_n\}}^{-1}=\overline{\{a_nb_n^{-1}\}}.$$

易知上面定义的运算是合理的, 然后在 $\widehat{F}$ 上定义赋值 $\widehat{\varphi}$ 如下：

$$\widehat{\varphi}(\{a_n\})=\lim_{n\to\infty}\varphi(a_n),$$

则易知 $\widehat{\varphi}$ 是合理的且满足：$\forall\alpha,\beta\in\widehat{F}$

(1) $\widehat{\varphi}(\alpha)\geqslant 0,\ \ \widehat{\varphi}(\alpha)=0\iff\alpha=\overline{\{0\}}$;

(2) $\widehat{\varphi}(\alpha\beta)=\widehat{\varphi}(\alpha)\widehat{\varphi}(\beta)$;

(3) $\widehat{\varphi}(\alpha+\beta)\leqslant\widehat{\varphi}(\alpha)+\widehat{\varphi}(\beta)$.

因此 $\widehat{\varphi}$ 确实是 $\widehat{F}$ 上的一个赋值, 且 $\widehat{\varphi}|_{\mathbb{Q}}=\varphi$(其中 $\mathbb{Q}\hookrightarrow\widehat{F}:a\mapsto\overline{\{a\}}$).

下证 $(\widehat{F},\widehat{\varphi})$ 是一个完备的赋值域. 设 $\{\alpha_l\}_{l=1}^{\infty}$ 是 $\widehat{F}$ 中一个柯西序列, 要证存在 $\alpha\in\widehat{F}$, 使得 $\widehat{\varphi}(\alpha_l-\alpha)\to 0$ (当 $l\to\infty$ 时). 因 $\alpha_l\in\widehat{F}$, 故存在 $\mathbb{Q}$ 中柯西序列 $\{a_n^{(l)}\}_{n=1}^{\infty}$, 使得 $\alpha_l=\{a_n^{(l)}\}_{n=1}^{\infty}$, 故存在 $n_0(l)$, 使得当 $n\geqslant n_0(l)$ 时, 有

$$\widehat{\varphi}(\alpha_l-a_n^{(l)})<\frac{1}{l}.$$

下证 $\alpha=\{a_{n_0(l)}^{(l)}\}_{l=1}^{\infty}$ 是 $\mathbb{Q}$ 上的柯西序列, 故 $\alpha\in\widehat{F}$, 且 $\alpha_l\to\alpha$. 事实上,

$$\begin{aligned}\varphi\big(a_{n_0(l)}^{(l)}-a_{n_0(l')}^{(l')}\big)&\leqslant\widehat{\varphi}\big(a_{n_0(l)}^{(l)}-\alpha_l\big)+\widehat{\varphi}\big(\alpha_l-\alpha_{l'}\big)+\widehat{\varphi}\big(\alpha_{l'}-a_{n_0(l')}^{(l')}\big)\\&\leqslant\frac{1}{l}+\widehat{\varphi}(\alpha_l-\alpha_{l'})+\frac{1}{l'}\to 0,\end{aligned}$$

又

$$\widehat{\varphi}(\alpha_l-\alpha)\leqslant\widehat{\varphi}\big(\alpha_l-a_{n_0(l)}^{(l)}\big)+\widehat{\varphi}\big(a_{n_0(l)}^{(l)}-\alpha\big)\to 0\quad(当\ l\to\infty\ 时),$$

故 $\alpha_l\to\alpha$, 从而 $(\widehat{F},\widehat{\varphi})$ 是完备的赋值域.

又由 $(\widehat{F},\widehat{\varphi})$ 的构造知 $\mathbb{Q}$ 在 $\widehat{F}$ 中是稠密的, 证毕.

定义 6.7 (1) 当 $\varphi=|\cdot|$ 时, 上面定理中的 $(\widehat{F},\widehat{\varphi})=(\mathbb{R},|\cdot|)$;

(2) 当 $\varphi=|\cdot|_p$ 时, 上面定理中的 $(\widehat{F},\widehat{\varphi})$ 为 p-adic 数域, 记为 $\mathbb{Q}_p$.

下面求出 $\mathbb{Q}_p$ 中每个元素的具体表达式：

(a) 先研究有理数 $a/b,(a,b)=1,p\nmid b$ 的 p-adic 表示法. 为此研究同余式

$$bx\equiv a\pmod{p^l}\qquad(0\leqslant x<p^l)$$

的解, 设其解为 x_l, 则 $p^l|(bx_l-a)$, 从而

$$\left|\frac{a}{b}-x_l\right|_p \leqslant p^{-l},$$

进而 $x_l \to \frac{a}{b}$(关于 $|\cdot|_p$), 故 $\frac{a}{b}=\lim\limits_{l\to\infty} x_l$.

在 §6.1 中已定义

$$x_l = a_0 + a_1 p + \cdots + a_{l-1}p^{l-1}, \qquad 0 \leqslant a_i < p,$$

由于

$$\begin{aligned}\varphi(x_l - x_{l'}) &= \varphi(a_l p^l + \cdots + a_{l'-1}p^{l'-1}) \\ &\leqslant p^{-l}\varphi(a_l) + \cdots + p^{-(l'-1)}\varphi(a_{l'-1}) \\ &\leqslant p^{-l} + \cdots + p^{-(l'-1)} = \frac{\frac{1}{p^l} - \frac{1}{p^{l'}}}{1-\frac{1}{p}} \to 0,\end{aligned}$$

从而 $\{x_l\}_{l=1}^{\infty}$ 是一柯西序列, 故 $\{x_l\}_{l=1}^{\infty} \in \mathbb{Q}_p$, 进而由它就得到有理数 a/b $(p \nmid b)$ 的 p-adic 表达式

$$a_0 + a_1 p + \cdots + a_{l-1}p^{l-1} + \cdots, \qquad 0 \leqslant a_i < p.$$

(b) 其次可得有理数 a/b, $(a,b)=1$, $p^m \| b(m \geqslant 0$ 为整数$)$ 的 p-adic 表达式为

$$p^{-m}(a_0 + a_1 p + \cdots + a_l p^l + \cdots), \qquad 0 \leqslant a_i < p, \quad m \geqslant 0, \tag{6.7}$$

这就是有理数表为 p-adic 数的一般形式.

如果在 (6.7) 式中, 有

$$a_{l+v} = a_{l+v+t} = a_{l+v+2t} = \cdots = a_{l+v+nt} = \cdots \qquad (v = 1, 2, \cdots, t),$$

这里 l 和 t 为固定的整数, $t \geqslant 1$, 则称 (6.7) 式是循环的, 此时可改写为

$$\begin{aligned}&p^{-m}\big[(a_0 + \cdots + a_l p^l) + p^{l+1}(a_{l+1} + a_{l+2}p + \cdots + a_{l+t}p^{t-1}) \\ &\quad + p^{l+t+1}(a_{l+1} + a_{l+2}p + \cdots + a_{l+t}p^{t-1}) + \cdots\big] \\ &= p^{-m}(A + p^{l+1}B + p^{l+t+1}B + p^{l+2t+1}B + \cdots),\end{aligned}$$

其中 $A = a_0 + \cdots + a_l p^l$, $B = a_{l+1} + a_{l+2}p + \cdots + a_{l+t}p^{t-1}$.

定理 6.7 有理数的 p-adic 表达式是 p 的循环幂级数, 反之, p 的循环幂级数是有理数.

证明 (1) 若

$$\alpha = p^{-m}(A + p^{l+1}B + p^{l+t+1}B + p^{l+2t+1}B + \cdots),$$

则

$$\alpha p^m - A = p^{l+1}B(1 + p^t + p^{2t} + \cdots) = p^{l+1}B \cdot \frac{1}{1-p^t},$$

即

$$\alpha = p^{-m}A + p^{l+1-m}B \cdot \frac{1}{1-p^t} \in \mathbb{Q}.$$

(2) 先讨论有理数

$$\alpha = \frac{r}{s}, \quad |\alpha| < 1, \quad (r,s) = 1, \quad s > 0, \quad r < 0, \quad p \nmid s.$$

设 t 是适合 $p^t \equiv 1 \pmod{s}$ 的最小正整数, 令

$$1 - p^t = ms, \quad m < 0,$$

则 $\alpha = \frac{r}{s} = \frac{mr}{1-p^t}$.

由于 $|\alpha| < 1$, 故 $mr = b_0 + b_1 p + \cdots + b_{t-1}p^{t-1}$ $(0 \leqslant b_i < p)$, 于是

$$\begin{aligned}\alpha &= (b_0 + b_1 p + \cdots + b_{t-1}p^{t-1})(1 + p^t + p^{2t} + \cdots) \\ &= (b_0 + \cdots + b_{t-1}p^{t-1}) + p^t(b_0 + \cdots + b_{t-1}p^{t-1}) + \cdots,\end{aligned}$$

即 α 是循环的 p 的幂级数.

其次, 设 $\alpha = a/b$, $(a,b) = 1$, $p^m \| b$ 为任意正有理数, 则

$$p^m\alpha = a_0 + a_1 p + \cdots + a_v p^v + \frac{r}{s}, \qquad 0 \leqslant a_i < p,$$

其中 $\frac{r}{s}$ 或为 0 或适合上面已讨论过的条件.

若 $-\alpha$ 为负有理数, 则先求出 α 的表达式, 再求

$$0 = p + (p-1)p + (p-1)p^2 + \cdots$$

与 α 的差, 即得 $-\alpha$ 的表达式, 而且所得的 p 的幂级数也是循环的, 证毕.

有理数的表示法如上, 再来解决一般情形. 首先由 $\mathbb{Q}_p$ 的定义易知

$$\alpha = p^{-m}(a_0 + a_1 p + \cdots a_l p^l + \cdots), \qquad 0 \leqslant a_i < p, \ m \geqslant 0$$

是 $\mathbb{Q}_p$ 中的元素 ($\because \{x_l\} = \{(a_0 + a_1 p + \cdots a_l p^l)p^{-m}\}$ 是柯西序列).

下证任意一个 $\alpha \in \mathbb{Q}_p$ 均有如上形式的表达式. 设 $\alpha = \{a_l\}_{l=1}^{\infty} \in \mathbb{Q}_p$, 其中 $a_l \in \mathbb{Q}$ 且 $\{a_l\}$ 是关于 $|\cdot|_p$ 的柯西序列, 由前知 a_l 有 p-adic 表达式

$$a_l = p^{-m_l}(a_0^{(l)} + a_1^{(l)}p + \cdots), \qquad 0 \leqslant a_i^{(l)} < p,$$

对任一正整数 t, 存在正整数 L, 使得当 $l, l' > L$ 时, 有

$$|a_l - a_{l'}|_p < \frac{1}{p^t}.$$

这表明, 当 $l > L$ 时, $a_l, a_{l+1}, a_{l+2}, \cdots$ 表示 p 的幂级数时, 其前面 $t+k$ 项 (k 非负整数) 必须相同. 由于 t 可以任意大, 令 $t \to \infty$, 可知 α 一定具有形式 $p^{-m}(a_0 + a_1p + \cdots)$ 的表达式.

因此我们证明了 $\mathbb{Q}_p$ 的全体即 $p^{-m}(a_0 + a_1p + \cdots + a_lp^l + \cdots)$ 的全体.

§6.4　Hensel 引理

定理 6.8 (Hensel)　设 $f(x)$ 是一整系数多项式, 且

$$f(x) \equiv g_0(x)h_0(x) \pmod p,$$

此处 g_0 和 h_0 为互素的多项式, 则存在 $g(x), h(x) \in \mathbb{Z}_p[x]$, 使得 $g(x) \equiv g_0(x)$, $h(x) \equiv h_0(x) \pmod p$ 且

$$f(x) = g(x)h(x).$$

证明　令 g_l 和 h_l 为两个多项式, 适合

$$g_l(x) \equiv g_0(x), \quad h_l(x) \equiv h_0(x) \pmod p, \quad 及 \quad f(x) \equiv g_l(x)h_l(x) \pmod{p^l}.$$

显然 g_l 和 h_l 互素 $(\mathrm{mod}\ p)$, 令

$$g_{l+1}(x) = g_l(x) + p^l\Phi(x), \qquad h_{l+1}(x) = h_l(x) + p^l\Psi(x),$$

则

$$g_{l+1}(x)h_{l+1}(x) \equiv g_l(x)h_l(x) + p^l(\Phi(x)h_l(x) + \Psi(x)g_l(x)) \pmod{p^{l+1}},$$

令

$$\frac{f(x) - g_l(x)h_l(x)}{p^l} \equiv t(x) \pmod p.$$

由于 h_l 与 g_l 互素 (mod p), 故存在两个多项式 $\varphi(x)$ 及 $\psi(x)$, 使得

$$t(x) \equiv \varphi(x)h_l(x) + \psi(x)g_l(x) \pmod p,$$

从而

$$\begin{aligned} f(x) - g_{l+1}(x)h_{l+1}(x) &\equiv f(x) - g_l(x)h_l(x) - p^l(\varphi(x)h_l(x) + \psi(x)g_l(x)) \\ &\equiv p^l(t(x) - \varphi(x)h_l(x) - \psi(x)g_l(x)) \equiv 0 \pmod{p^{l+1}}. \end{aligned}$$

由于 $\deg(t) \leqslant \deg(g_lh_l)$, 故可假定 $\deg(\varphi) \leqslant \deg(g_l), \deg(\psi) \leqslant \deg(h_l)$. 现在有多项式序列 $\{g_l(x)\}_{l=1}^{\infty}, \{h_l(x)\}_{l=1}^{\infty}$, $\deg(g_l) \leqslant \deg(g_0)$, $\deg(h_l) \leqslant \deg(h_0)$, 且显然 $\{g_l(x)\}$ 与 $\{h_l(x)\}$ 的系数成柯西序列, 因此它们收敛到 $\mathbb{Z}_p$ 中的某些数, 从而 $g_l(x) \to g(x)$, $h_l(x) \to h(x)$, 而

$$f(x) = g(x)h(x).$$

证毕.

例 6.6 试证明 $\mathbb{Q}_p$ 中共有 $p-1$ 个不同的 $p-1$ 次单位根.

证明 多项式 $f(x) = x^{p-1} - 1$ 在 $\mathbb{Z}/p\mathbb{Z}$ 中分解成 $p-1$ 个 1 次因子之积:

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-(p-1)) \pmod p.$$

由 Hensel 引理可知: 对每个整数 a, $1 \leqslant a \leqslant p-1$, 均有 $\varepsilon_a \in \mathbb{Q}_p$, 使得

$$\varepsilon_a^{p-1} = 1 \quad \text{且} \varepsilon_a \equiv a \pmod p,$$

于是对不同的 a 给出不同的 ε_a, 它们均是 $p-1$ 次单位根.

例 6.7 设 p 为素数, $a \in \mathbb{Z}$, $p \nmid a$, 求证在 $\mathbb{Q}_p$ 中极限 $\lim_{n\to\infty} a^{p^n}$ 存在, 记之为 ε_a $(1 \leqslant a \leqslant p-1)$, 求证 ε_a 恰好是 $\mathbb{Q}_p$ 中 $p-1$ 个 $p-1$ 次单位根.

证明 序列 $\{a^{p^n}\}_{n=1}^{\infty}$ 为柯西序列: $\forall m > n \geqslant N$,

$$\left|a^{p^m} - a^{p^n}\right|_p = \left|a^{p^n}(a^{p^m - p^n} - 1)\right|_p = \left|a^{p^m-p^n} - 1\right|_p \leqslant p^{-N} \to 0.$$

从而极限 $\lim_{n\to\infty} a^{p^n}$ 在 $\mathbb{Q}_p$ 中存在, 设为 ε_a, 则

$$\varepsilon_a^{p-1} = \left(\lim_{n\to\infty} a^{p^n}\right)^{p-1} = \lim_{n\to\infty} \left(a^{p^n}\right)^{p-1} = \lim_{n\to\infty} \left(a^{p-1}\right)^{p^n} = 1.$$

可见 ε_a 是 $\mathbb{Q}_p$ 中 $p-1$ 次单位根, 又易知

$$\varepsilon_a \equiv a \pmod p,$$

故 $\varepsilon_a \neq \varepsilon_b$, $\forall a \neq b, 1 \leqslant a, b \leqslant p-1$.

为了将来的应用, 我们叙述 Hensel 引理的一个更一般的形式:

定理 6.9 (Hensel)　设 R 是一个环, 它关于其某个理想 $I \subset R$ 是完备的, 且设 $F(w) \in R[w]$ 是一个多项式. 假定 $a \in R$ 满足

$$F(a) \in I^n, \text{ 且} F'(a) \in R^*,$$

则对于任意的 $\alpha \in R$, 若 $\alpha \equiv F'(a)((\bmod\ I))$, 则序列

$$w_0 = a, w_{m+1} = w_m - F(w_m)/\alpha$$

收敛到 R 中一个元素 $b \in R$, 且满足

$$F(b) = 0 \text{ 且 } b \equiv a(\ (\bmod\ I^n)).$$

又若 R 是一个整环, 则这些条件惟一决定元素 b.

证明　为了简化记号, 用 $F(w+a)/\alpha$ 代替 $F(w)$, 从而可以假定我们的递归序列为

$$w_0 = 0, \quad F(0) \in I^n, \quad F'(0) \equiv 1(\ (\bmod\ I)), \quad w_{m+1} = w_m - F(w_m).$$

由于 $F(0) \in I^n$, 因此, 若 $w_m \in I^n$, 则 $w_m - F(w_m) \in I^n$, 于是

$$w_m \in I^n, \quad \forall m \geqslant 0.$$

归纳地证明

$$w_m \equiv w_{m+1}((\bmod\ I^{m+n})), \quad \forall m \geqslant 0.$$

对于 $m = 0$, 这就是说 $F(0) \equiv 0((\bmod\ I^n))$, 这是我们的原始假定. 现在设同余式对所有小于 m 的整数都成立, 令 X 和 Y 是新的变量, 分解

$$F(X) - F(Y) = (X - Y)(F'(0) + XG(X,Y) + YH(X,Y)),$$

其中多项式 $G(X,Y), H(X,Y) \in R[X,Y]$. 于是

$$\begin{aligned}
w_{m+1} - w_m &= (w_m - F(w_m)) - (w_{m-1} - F(w_{m-1})) \\
&= (w_m - w_{m-1}) - (F(w_m) - F(w_{m-1})) \\
&= (w_m - w_{m-1})[1 - F'(0) - w_m G(w_m, w_{m-1}) \\
&\quad - w_{m-1} H(w_m, w_{m-1})] \in I^{m+n},
\end{aligned}$$

此处, 最后的包含关系由归纳假设和事实 $F'(0) \equiv 1((\bmod\ I))$ 及 $w_m, w_{m-1} \in I^n$ 得出. 这就证明了 $w_m - w_{m-1} \in I^{m+n}$(对所有的 $m \geqslant 0$).

由于 R 关于 I 是完备的, 可知序列 w_m 收敛到 R 的一个元素 b, 又因 $w_m \in I^n$, 故 $b \in I^n$, 更进一步, 在关系式 $w_{m+1} = w_m - F(w_m)$ 中令 $m \to \infty$, 取极限就得到 $b = b - F(b)$, 即 $F(b) = 0$.

最后, 为了证明惟一性 (假定 R 是整环), 设还存在 $c \in I^n$, 使得 $F(c) = 0$, 则

$$0 = F(b) - F(c) = (b - c)(F'(0) + bG(b, c) + cH(b, c)).$$

若 $b \neq c$, 则 $F'(0) + bG(b, c) + cH(b, c) = 0$, 但是 $bG(b, c) + cH(b, c) \in I$, 所以 $F'(0) \in I$, 这与假设 $F'(0) \equiv 1((\bmod\ I))$ 矛盾. 因此, $b = c$. 证毕.

第七章　椭圆曲线的形式群

§7.1　在无穷远点展开

在本节中, 我们讨论椭圆曲线及其运算在无穷远点附近的结构. 做变量替换:

$$z=-\frac{x}{y},\qquad w=-\frac{1}{y}\qquad \Big(\text{即 } x=\frac{z}{w},\ y=-\frac{1}{w}\Big), \tag{7.1}$$

于是 E 上的无穷远点 $\mathcal{O}=[0,1,0]$ 变为点 $(z,w)=(0,0)$, 并且 z 是 E 在 $\mathcal{O}$ 处的局部一致化子 (即 z 在 $\mathcal{O}$ 处有 1 阶零点). 于是 E 的方程变为

$$w=z^3+a_1zw+a_2z^2w+a_3w^2+a_4zw^2+a_6w^3=f(z,w). \tag{7.2}$$

现在不断递归代入, 有

$$\begin{aligned} w &= z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3 \\ &= z^3+(a_1z+a_2z^2)\big(z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3\big) \\ &\quad +(a_3+a_4z)\big(z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3\big)^2 \\ &\quad +a_6\big(z^3+(a_1z+a_2z^2)w+(a_3+a_4z)w^2+a_6w^3\big)^3 \\ &= \cdots \\ &= z^3+a_1z^4+(a_1^2+a_2)z^5+(a_1^3+2a_1a_2+a_3)z^6 \\ &\quad +(a_1^4+3a_1^2a_2+3a_1a_3+a_2^2+a_4)z^7+\cdots \\ &= z^3(1+A_1z+A_2z^2+\cdots), \end{aligned} \tag{7.3}$$

此处 $A_n\in\mathbb{Z}[a_1,a_2,\cdots,a_6]$, 上述过程可精确描述如下:

$$f_1(z,w)=f(z,w),\quad f_{m+1}(z,w)=f_m(z,f(z,w)),$$

然后令

$$w(z)=\lim_{m\to\infty}f_m(z,0),$$

只要该极限在 $\mathbb{Z}[a_1,\cdots,a_6][[z]]$ 中有意义.

定理 7.1 (a) 上述过程给出了一个幂级数

$$w(z) = z^3(1 + A_1 z + A_2 z^2 + \cdots) \in \mathbb{Z}[a_1, \cdots, a_6][[z]];$$

(b) $w(z)$ 是惟一满足 $w(z) = f(z, w(z))$ 的幂级数;

(c) 若 $\mathbb{Z}[a_1, \cdots, a_6]$ 通过令 $\mathrm{wt}(a_i) = i$ 作成一个分次环, 则 A_n 是权 n 的齐次多项式.

证明 (a) 和 (b) 是 Hensel 引理 (定理 6.9) 的一个特殊情形, 我们取

$$R = \mathbb{Z}[a_1, \cdots, a_6][[z]], I = (z),$$
$$F(w) = f(z, w) - w, a = 0, \alpha = -1.$$

为了证明 (c), 赋予 z 和 w 权如下:

$$\mathrm{wt}(z) = -1, \quad \mathrm{wt}(w) = -3,$$

则 $f(z, w)$ 是分次环 $\mathbb{Z}[a_1, \cdots, a_6]$ 中的权为 -3 的齐次多项式, 由归纳法, 易知每个 $f_m(z, w)$ 都是权为 -3 的齐次多项式, 特别地,

$$f_m(z, 0) = z^3(1 + B_1 z + B_2 z^2 + \cdots + B_N z^N)$$

是权为 -3 的齐次多项式, 因此, 每个 B_n 是分次环 $\mathbb{Z}[a_1, \cdots, a_6]$ 中权为 n 的齐次多项式. 因而 A_n 亦如此 (因 $w(z) = \lim_{m\to\infty} f_m(z, 0) = z^3(1 + A_1 z + A_2 z^2 + \cdots)$). 这就完成了证明.

利用 (7.2) 和 (7.3) 式, 得出 x 和 y 的 Laurent 级数

$$x(z) = \frac{z}{w(z)} = \frac{1}{z^2} - \frac{a_1}{z} - a_2 - a_3 z - (a_4 + a_1 a_3) z^2 - \cdots,$$
$$y(z) = \frac{-1}{w(z)} = -\frac{1}{z^3} + \frac{a_1}{z^2} + \frac{a_2}{z} + a_3 + (a_4 + a_1 a_3) z + \cdots.$$

类似地, 不变微分有表达式为

$$\omega(z) = \big(1 + a_1 z + (a_1^2 + a_2) z^2 + (a_1^3 + 2a_1 a_2 + 2a_3) z^3 + (a_1^4 + 3a_1^2 a_2 + 6a_1 a_2 + a_2^2 + 2a_4) z^4 + \cdots\big) dz.$$

上述 $x(z)$ 和 $y(z)$ 及 $\frac{\omega(z)}{dz}$ 的系数 $\in \mathbb{Z}[a_1, \cdots, a_6]$.

于是有序对 $\big(x(z), y(z)\big)$ 提供了 E 的一个"形式解", 即一个在形式幂级数域中的解, 特别地, 如果 K 是一个完备局部域, R 为其整数环, $\mathcal{M}$ 是 R 的极大理想, 且系数 $a_i \in R$, 则 $\forall z \in \mathcal{M}$, 幂级数 $x(z)$ 和 $y(z)$ 均收敛, 从而给出一个点 $\big(x(z), y(z)\big) \in E(K)$, 于是得到一个单射 (其逆为 $z = -x(z)/y(z)$)

$$\begin{aligned} \mathcal{M} &\longrightarrow E(K) \\ z &\longmapsto \big(x(z), y(z)\big), \end{aligned}$$

该映射将是我们的主要工具之一.

现在回到形式幂级数, 主要找出相应于 E 上加法的表达式. 设 z_1 和 z_2 是两个不定元, $w_i = w(z_i)$, $i = 1, 2$, 在 (z, w) 平面上, 连结 (z_1, w_1) 和 (z_2, w_2) 的直线斜率为

$$\lambda = \lambda(z_1, z_2) = \frac{w_2 - w_1}{z_2 - z_1} = \sum_{n=3}^{\infty} A_n \frac{z_2^n - z_1^n}{z_2 - z_1} \in \mathbb{Z}[a_1, \cdots, a_6][[z_1, z_2]],$$

置

$$v = v(z_1, z_2) = w_1 - \lambda z_1 \in \mathbb{Z}[a_1, \cdots, a_6][[z_1, z_2,]].$$

于是直线方程为 $w = \lambda z + v$, 代入 (7.2) 式, 得出 z 的一个 3 次方程, 已知其两个根为 z_1 和 z_2, 设第 3 个根为 z_3, 利用韦达定理知

$$\begin{aligned} z_3 &= z_3(z_1, z_2) \\ &= -z_1 - z_2 + \frac{a_1\lambda + a_3\lambda^2 - a_2 v - 2a_4\lambda v - 3a_6\lambda^2 v}{1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3} \in \mathbb{Z}[a_1, \cdots, a_6][[z_1, z_2]]. \end{aligned}$$

注意到 (z_1, w_1)、(z_2, w_2) 和 (z_3, w_3) 之和为 $\mathcal{O}$, 故为了求 $(z_1, w_1) + (z_2, w_2)$, 我们要求出逆的公式, 在 (x, y) 平面上, (x, y) 的逆为 $(x, -y - a_1x - a_3)$, 故 (z, w) 的逆的 z 坐标 (注意 $z = -x/y$)

$$i(z) = \frac{x(z)}{y(z) + a_1x(z) + a_3} = \frac{z^{-2} - a_1z^{-1} - \cdots}{-z^{-3} + 2a_1z^{-2} + \cdots} \in \mathbb{Z}[a_1, \cdots, a_6][[z]].$$

于是得出形式加法的规律:

$$\begin{aligned} F(z_1, z_2) &= i(z_3(z_1, z_2)) \\ &= z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) - (2a_3z_1^3z_2 - (a_1a_2 - 3a_3)z_1^2z_2^2 \\ &\quad + 2a_3z_1z_2^3) + \cdots \in \mathbb{Z}[a_1, \cdots, a_6][[z_1, z_2]]. \end{aligned}$$

由椭圆曲线 E 的性质易知 $F(z_1, z_2)$ 有以下性质:

$$\begin{aligned} F(z_1, z_2) &= F(z_2, z_1) && \text{(交换律)}, \\ F(z_1, F(z_2, z_3)) &= F(F(z_1, z_2), z_3) && \text{(结合律)}, \\ F(z, i(z)) &= 0 && \text{(逆元)}. \end{aligned}$$

§7.2　形　式　群

定义 7.1　设 R 是一个环, R 上的一个 (单参数交换) 形式群 $\mathcal{F}$ 是一幂级数 $F(X, Y) \in R[[X, Y]]$, 满足

(a) $F(X,Y) = X + Y +$ 高次项;

(b) $F(X, F(Y,Z)) = F(F(X,Y),Z)$;

(c) $F(X,Y) = F(Y,X)$;

(d) 存在惟一的幂级数 $i(T) \in R[[T]]$, 使得 $F(T, i(T)) = 0$;

(e) $F(X,0) = X$, $F(0,Y) = Y$.

则称 $F(X,Y)$ 是 $\mathcal{F}$ 的形式群律.

于是可知伴随到椭圆曲线 E 的 $F(z_1, z_2)$ 是一个形式群. 从形式群 $\mathcal{F}$ 到形式群 $\mathcal{G}$ 的同态是一个幂级数 $f(T) \in R[[T]]$, 它满足

$$f(F(X,Y)) = G(f(X), f(Y)).$$

若存在同态 $f: \mathcal{F} \to \mathcal{G}$ 及 $g: \mathcal{G} \to \mathcal{F}$, 使得

$$f(g(T)) = g(f(T)) = T,$$

则称 $\mathcal{F}$ 和 $\mathcal{G}$ 是同构的.

例 7.1 设 $(\mathcal{F}, F)$ 是形式群, 归纳定义同态如下:

$$[m]: \mathcal{F} \to \mathcal{F},$$

$[0](T) = 0$, $[m+1](T) = F([m](T), T)$, $[m-1](T) = F([m](T), i(T))$. 易知 $[m]$ 是一个同态, 称为 m 倍乘映射.

定理 7.2 设 $\mathcal{F}$ 是 R 上的形式群, $m \in \mathbb{Z}$, 则

(a) $[m]T = mT \ + \ $ 高次项;

(b) 若 $m \in R^*$, 则 $[m]: \mathcal{F} \to \mathcal{F}$ 是同构.

证明 (a) 对 $m \geqslant 0$, 归纳证之 (利用 $F(X,Y) = X + Y +$ 高次项), 又

$$0 = F(T, i(T)) = T + i(T) + \text{高次项},$$

$\Longrightarrow i(T) = -T +$ 高次项, 然后归纳证明 $m < 0$ 的情形.

(b) 可以从 (a) 和下述引理得知, 证毕.

引理 7.1 设 $a \in R^*, f(T) \in R[[T]]$ 为一幂级数, 且

$$f(T) = aT \ + \ \text{高次项},$$

则存在惟一幂级数 $g(T) \in R[[T]]$, 使得 $f(g(T)) = g(f(T)) = T$.

证明 构造多项式序列 $g_n(T) \in R[T]$, 使得

$$f(g_n(T)) \equiv T \pmod{T^{n+1}}, \qquad g_{n+1} \equiv g_n(T) \pmod{T^{n+1}},$$

第 1 步, 取 $g_1(T) = a^{-1}T$, 设 $g_{n-1}(T)$ 已找到, 寻找 $\lambda \in R$, 使得

$$g_n(T) = g_{n-1}(T) + \lambda T^n$$

有要求的性质. 计算

$$\begin{aligned} f(g_n(T)) &= f\big(g_{n-1}(T) + \lambda T^n\big) \equiv f\big(g_{n-1}(T)\big) + a\lambda T^n \pmod{T^{n+1}} \\ &\equiv T + bT^n + a\lambda T^n \pmod{T^{n+1}}. \end{aligned}$$

对某个 $b \in R\,(\because f(g_{n-1}(T)) \equiv T \pmod{T^n})$, 取 $\lambda = -b/a \in R$, 则

$$f(g_n(T)) \equiv T \pmod{T^{n+1}}, \qquad g_n(T) \equiv g_{n-1}(T) \pmod{T^n}.$$

取极限知 $g(T) = \lim g_n(T)$ 存在, 且 $f(g(T)) = T$, 从而

$$g(f(g(T))) = g(T).$$

这是在幂级数环 $R[[g(T)]]$ 中的恒等式, 故 $g(f(T)) = T$, 证毕.

下面总设 R 是一个完备局部环 (例如 $R = \mathbb{Z}_p$ 为 p-adic 整数环), $\mathcal{M}$ 是 R 的极大理想, $k = R/\mathcal{M}$ 是剩余类域, K 是 R 的分式域, $(\mathcal{F}, F)$ 是 R 上的形式群.

定义 7.2 伴随到 $\mathcal{F}/R$ 的群, 记为 $\mathcal{F}(\mathcal{M})$, 它是集合 $\mathcal{M}$ 及群律

$$\begin{aligned} &x \oplus_{\mathcal{F}} y = F(x, y), \quad \forall x, y \in \mathcal{M}, \\ &\ominus_{\mathcal{F}} x = i(x), \qquad\quad \forall x \in \mathcal{M}. \end{aligned}$$

类似地, 对 $n \geqslant 1$, $\mathcal{F}(\mathcal{M}^n)$ 是 $\mathcal{F}(\mathcal{M})$ 的子群, 其集合为 $\mathcal{M}^n$.

例 7.2 设 E/K 是椭圆曲线, $\widehat{E}$ 是其伴随形式群, 于是幂级数 $x(z)$ 和 $y(z)$ 给出了一个映射

$$\begin{aligned} \mathcal{M} &\longrightarrow E(K) \\ z &\longmapsto \big(x(z), y(z)\big). \end{aligned}$$

由 $\widehat{E}$ 的定义, 该映射给出了 $\widehat{E}(\mathcal{M})$ 到 $E(K)$ 的一个同态, 我们将看到, 存在一个正合列

$$0 \to \widehat{E}(\mathcal{M}) \to E(K) \to \widetilde{E}(k) \to 0,$$

此处 $\widetilde{E}$ 是定义在剩余类域 $k = R/\mathcal{M}$ 上的椭圆曲线, 从而 $E(K)$ 的研究就归结为形式群 $\widehat{E}$ 和一个更小的域 k(通常是有限域) 上椭圆曲线的研究.

定理 7.3 (a) 对每一个 $n \geqslant 1$, 映射

$$\begin{aligned} \mathcal{F}(\mathcal{M}^n)/\mathcal{F}(\mathcal{M}^{n+1}) &\longrightarrow \mathcal{M}^n/\mathcal{M}^{n+1} \\ x &\longmapsto x \end{aligned}$$

是群同构;

(b) 设 $p = \mathrm{ch}(k)$, 则 $\mathcal{F}(\mathcal{M})$ 的每个扭元 (torsion) 的阶为 p 的幂次.

证明 (a) 因集合是同一个, 因此只要证映射是同态即可. $\forall x, y \in \mathcal{M}^n$, 有

$$x \oplus_{\mathcal{F}} y = F(x, y) = x + y + \text{高次项} \equiv x + y \pmod{\mathcal{M}^{2n}}.$$

(b) 只要证明没有非零扭元, 其阶与 p 互素即可. 设 $m \geqslant 1$, $(m, p) = 1$, 且 $x \in \mathcal{F}(\mathcal{M})$, 使得 $[m](x) = 0$, 要证 $x = 0$.

因 $(m, p) = 1$, 所以 $m \notin \mathcal{M}$, 故 $m \in R^*$, 所以 $[m]$ 是形式群 $\mathcal{F}/R$ 上的同构, 从而它诱导出一个同构

$$[m] : \mathcal{F}(\mathcal{M}) \simeq \mathcal{F}(\mathcal{M}),$$

特别地, 其核为 0, 即 $x = 0$, 证毕.

定义 7.3 所谓 $\mathcal{F}/R$ 上的一个不变微分是指一个微分形式

$$\omega(T) = P(T)dT \in R[[T]]dT,$$

满足

$$\omega \circ F(T, S) = \omega(T),$$

换言之, 即满足

$$P\big(F(T, S)\big)F_X(T, S) = P(T),$$

其中 $F_X(X, Y)$ 是 F 关于第一个变元的偏导数. 若 $P(0) = 1$, 则称 $\omega(T)$ 是正规化不变微分.

定理 7.4 在 $\mathcal{F}/R$ 上存在惟一的正规化不变微分, 它由下述公式给出:

$$\omega = F_X(0, T)^{-1}dT,$$

每一个 $\mathcal{F}/R$ 上的不变微分均为 $a\omega$ 的形式, 对某个 $\alpha \in R$.

证明 设 $P(T)dT$ 是一个不变微分, 则

$$P\big(F(T, S)\big)F_X(T, S) = P(T).$$

令 $T=0$, 则

$$P(S)F_X(0,S)=P(0)\quad (\because F(0,S)=S),$$

但 $F_X(0,S)=1+\cdots$, 故 $P(S)$ 由 $P(0)$ 决定, 于是每一个可能的不变微分均具有形式 $a\omega$, $a\in R$, $\omega(T)=F_X(0,T)^{-1}dT$. 下证 $\omega(T)=F_X(0,T)^{-1}dT$ 是正规化不变微分, 正规化是显然的, 只要证

$$F_X\big(0,F(T,S)\big)^{-1}F_X(T,S)=F_X(0,T)^{-1}.$$

因为

$$F\big(U,F(T,S)\big)=F\big(F(U,T),S\big),$$

关于 U 微分, 得

$$F_X\big(U,F(T,S)\big)=F_X\big(F(U,T),S\big)F_X(U,T).$$

置 $U=0$, 注意 $F(0,T)=T$, 即得所要证的.

推论 7.1 设 $\mathcal{F},\mathcal{G}/R$ 为形式群, $\omega_{\mathcal{F}}$ 和 $\omega_{\mathcal{G}}$ 为相应的正规化不变微分, 设 $f:\mathcal{F}\to\mathcal{G}$ 是同态, 则

$$\omega_{\mathcal{G}}\circ f=f'(0)\omega_{\mathcal{F}}.$$

证明 设 $F(X,Y)$ 和 $G(X,Y)$ 是 $\mathcal{F}$ 和 $\mathcal{G}$ 的形式群律, 先证 $\omega_{\mathcal{G}}\circ f$ 是 $\mathcal{G}$ 上的不变微分:

$$\begin{aligned}\omega_{\mathcal{G}}\circ f\big(F(T,S)\big)&=\omega_{\mathcal{G}}\big(G(f(T),f(S))\big)\qquad (\text{因 } f \text{ 是同态})\\&=\omega_{\mathcal{G}}\circ f(T)\qquad (\text{因}\omega_{\mathcal{G}}\text{是不变微分, 故}\omega_{\mathcal{G}}\circ G(T,S)=\omega_{\mathcal{G}}(T)),\end{aligned}$$

可见 $\omega_{\mathcal{G}}\circ f$ 是 $\mathcal{F}$ 上的不变微分, 由定理 7.4, $\omega_{\mathcal{G}}\circ f=a\omega_{\mathcal{F}}$, 比较第一项, 知 $a=f'(0)$, 证毕.

推论 7.2 设 $\mathcal{F}/R$ 是形式群, $p\in\mathbb{Z}$ 为素数, 则存在幂级数 $f(T)$, $g(T)\in R[[T]]$, 使得

$$[p](T)=pf(T)+g(T^p).$$

证明 设 $\omega(T)$ 是 $\mathcal{F}$ 的正规化不变微分, 则由定理 7.2 知 $[p]'(0)=p$, 于是由推论 7.1, 知

$$p\omega(T)=\omega\circ[p](T)=(1+\cdots)[p]'(T)dT.$$

因 $(1+\cdots)$ 在 $R[[T]]$ 中可逆, 故 $[p]'(T)\in pR[[T]]$, 从而 $[p](T)$ 中每个项 aT^n 满足 $a\in pR$ 或 $p|n$, 证毕.

例 7.3 设 E 是椭圆曲线, $\widehat{E}$ 是其伴随的形式群, 于是其形式群律为

$$
\begin{aligned}
F(X,Y)=&X+Y-a_1XY-a_2(X^2Y+XY^2)\\
&-(2a_3X^3Y-(a_1a_2-3a_3)X^2Y^2+2a_3XY^3)+\cdots,
\end{aligned}
$$

于是由 $[m](T)=F([m-1](T),T)$ 的定义知

$$
\begin{aligned}
[2](T)&=F(T,T)=2\{T-a_2T^3+\cdots\}+\{-a_1T^2+(a_1a_2-7a_3)T^4+\cdots\},\\
[3](T)&=F([2]T,T)=3\{T-a_1T^2+(4a_1a_2-13a_3)T^4+\cdots\}\\
&\quad+\{(a_1^2-8a_2)T^3+\cdots\}.
\end{aligned}
$$

定义 7.4 设 R 是一个特征 0 的环, $K=R\otimes\mathbb{Q}$, $\mathcal{F}/R$ 是一形式群, 设

$$\omega(T)=\left(1+c_1T+c_2T^2+c_3T^3+\cdots\right)dT$$

是其正规化不变微分, 则定义 $\mathcal{F}/R$ 的形式对数是幂级数

$$\log_{\mathcal{F}}(T)=\int\omega(T)=T+\frac{c_1}{2}T^2+\frac{c_2}{3}T^3+\cdots\in K[[T]].$$

而 $\mathcal{F}/R$ 的形式指数是惟一的幂级数 $\exp_{\mathcal{F}}(T)\in K[[T]]$, 它满足

$$\log_{\mathcal{F}}\circ\exp_{\mathcal{F}}(T)=\exp_{\mathcal{F}}\circ\log_{\mathcal{F}}(T)=T.$$

$\exp_{\mathcal{F}}$ 的存在惟一性是由引理 7.1 保证的.

例 7.4 设 $\mathcal{T}=\widehat{G}_m$ 是形式群 $F(X,Y)=X+Y+XY$, 则其正规化不变微分是

$$\omega(T)=F_X(0,T)^{-1}dT=(1+T)^{-1}dT \quad (\text{定理 } 7.4)$$

故

$$\log_{\mathcal{F}}(T)=\int(1+T)^{-1}dT=\sum_{n=1}^{\infty}\frac{(-1)^{n-1}T^n}{n},\qquad \exp_{\mathcal{F}}(T)=\sum_{n=1}^{\infty}\frac{T^n}{n!}.$$

定理 7.5 设 $\mathcal{F}/R$ 是形式群, $\mathrm{ch}(R)=0$, 则

$$\log_{\mathcal{F}}:\ \mathcal{F}\longrightarrow\widehat{G}_a$$

是形式群 (在 $K=R\otimes\mathbb{Q}$ 上) 的同构, 此处 $\widehat{G}_a$ 是形式群 $F_{\widehat{G}_a}(X,Y)=X+Y$.

证明　设 $\omega(T)$ 是 $\mathcal{F}/R$ 的正规不变微分, 即

$$\omega\big(F(T,S)\big)=\omega(T)$$

关于 T 积分, 得

$$\log_{\mathcal{F}} F(T,S)=\log_{\mathcal{F}}(T)+f(S),$$

其中 $f(S)\in K[[S]]$ 是积分常数. 令 $T=0$, 知 $f(S)=\log_{\mathcal{F}} F(0,S)=\log_{\mathcal{F}}(S)$, 故有

$$\log_{\mathcal{F}} F(T,S)=\log_{\mathcal{F}}(T)+\log_{\mathcal{F}}(S).$$

这说明 $\log_{\mathcal{F}}$ 是 $\mathcal{F}$ 到 $\widehat{G}_a$ 的同态, 又其逆是 $\exp_{\mathcal{F}}$, 故 $\log_{\mathcal{F}}$ 是同构, 证毕.

引理 7.2　设 $\mathrm{ch}(R)=0$, $f(T)=\sum_{n=1}^{\infty}\frac{a_n}{n!}T^n$, 使得 $a_i\in R$, $a_1\in R^*$, 则满足 $f\big(g(T)\big)=T$ 的惟一幂级数 $g(T)$ 能表达成

$$g(T)=\sum_{n=1}^{\infty}\frac{b_n}{n!}T^n,\qquad b_n\in R.$$

证明　因 $b_n=g^{(n)}(0)$, 故只需证 $g^{(n)}(0)\in R$. 由于 $f\big(g(T)\big)=T$, 微分得

$$f'\big(g(T)\big)g'(T)=1.$$

令 $T=0$, 得 $b_1=g'(0)=1/f'(0)=1/a_1\in R^*$, 再微分, 得

$$f'\big(g(T)\big)g''(T)+f''\big(g(T)\big)g'(T)^2=0.$$

重复微分证明 $\forall n\geqslant 2$, $f'\big(g(T)\big)g^{(n)}(T)$ 可表为 $f^{(i)}\big(g(T)\big)$ $(1\leqslant i\leqslant n)$ 和 $g^{(j)}$ $(1\leqslant j\leqslant n-1)$ 的多项式, 令 $T=0$, 则可知 a_1b_n 是 $a_1,\cdots,a_n$ 和 $b_1,\cdots,b_{n-1}$ 的多项式, 因 $a_1,b_1\in R^*$, 归纳易知 $b_n\in R$, 证毕.

推论 7.3　设 $\mathrm{ch}(R)=0$, 且 $\mathcal{F}/R$ 是一个形式群, 则

$$\log_{\mathcal{F}}(T)=\sum_{n=1}^{\infty}\frac{a_n}{n}T^n,\quad \text{且 } \exp_{\mathcal{F}}(T)=\sum_{n=1}^{\infty}\frac{b_n}{n!}T^n,\ a_n,b_n\in R,\quad \text{且 } a_1=b_1=1.$$

证明　$\log_{\mathcal{F}}$ 的表达式由其定义直接得出, 而 $\exp_{\mathcal{F}}$ 的表达式由引理 7.2 知.

下设 R 是完备局部环, $\mathcal{M}$ 是其极大理想, $\mathcal{F}/R$ 是一个形式群, 则其伴随群 $\mathcal{F}(\mathcal{M})$ 没有阶与 $p=\mathrm{ch}(R/\mathcal{M})$ 互素的扭元 (定理 7.3), 下面考虑 p 扭元.

定理 7.6　设 v 是 R 上的赋值, $\mathcal{F}/R$ 为形式群, $x\in\mathcal{F}(\mathcal{M})$ 的阶为 p^n($n\geqslant 1$ 即 $[p^n](x)=0$ 但 $[p^{n-1}](x)\neq 0$), 则

$$v(x)\leqslant\frac{v(p)}{p^n-p^{n-1}}.$$

证明 若 $\mathrm{ch}(R) \neq 0$ 或 $p = 0$, 则 $v(p) = \infty$, 定理自然成立, 下设不是如此, 由推论 7.2, 知

$$[p](T) = pf(T) + g(T^p),$$

其中 $f(T) = T + \cdots$, 下面归纳证明定理. 设 $x \neq 0, [p]x = 0$, 故

$$0 = pf(x) + g(x^p).$$

因 R 是离散赋值环, 故

$$v(px) \geqslant v(x^p)$$

(因若 $v(px) < v(x^p)$, 则 px 是 $pf(x) + g(x^p)$ 中赋值最小者, 从而 $v(0) = v(px)$, 矛盾), 即

$$v(x) \leqslant \frac{v(p)}{p-1}.$$

设定理对 n 成立, 设 $x \in \mathcal{F}(\mathcal{M})$ 恰有阶 p^{n+1}, 则

$$v\big([p](x)\big) = v\big(pf(x) + g(x^p)\big) \geqslant \min\{v(px), v(x^p)\},$$

但 $[p](x)$ 的阶为 p^n, 故由归纳假设知

$$\frac{v(p)}{p^n - p^{p-1}} \geqslant v\big([p](x)\big),$$

因此

$$\frac{v(p)}{p^n - p^{n-1}} \geqslant \min\{v(px), v(x^p)\}.$$

因 $v(x) > 0, n \geqslant 1$, 故

$$\frac{v(p)}{p^n - p^{n-1}} \geqslant v(px) = v(p) + v(x)$$

不可能 (否则 $v(x) < 0$), 从而

$$\frac{v(p)}{p^n - p^{n-1}} \geqslant v(x^p) = pv(x) \Longrightarrow v(x) \leqslant \frac{v(p)}{p^{n+1} - p^n}.$$

证毕.

例 7.5 设 $\mathcal{F}$ 是定义在 $\mathbb{Z}_p$ 上的形式群, 若 $p \geqslant 3$, 则定理 7.6 表明 $\mathcal{F}(p\mathbb{Z}_p)$ 根本没有扭元, 而对于 $p = 2$, 只能有 $n = 1$, 即最多有 2 阶扭元. 当然对于 $\mathbb{Q}_p$ 的任意有限不分歧扩域的整数环也成立.

下设 $\mathrm{ch}(R) = p > 0$.

定义 7.5　设 $\mathcal{F}, \mathcal{G}/R$ 是形式群, $f: \mathcal{F} \to \mathcal{G}$ 是定义在 R 上的同态, f 的高度 $(ht(f))$ 定义为最大整数 h, 使得

$$f(T) = g(T^{p^h}),$$

其中幂级数 $g(T) \in R[[T]]$, $ht(0) = \infty$. 而定义 $ht(\mathcal{F})$ 是映射 $[p]: \mathcal{F} \to \mathcal{F}$ 的高度, 即 $ht(\mathcal{F}) = ht([p])$.

例 7.6　若 $m \geqslant 1$, $(m, p) = 1$, 则 $ht([m]) = 0$, 这是因为由定理 7.2, 有 $[m](T) = mT + \cdots$; 另一方面推论 7.2 表明 $[p](T) = pf(T) + g(T^p) = g(T^p)$, 故 $ht([p]) \geqslant 1$. 从而一个形式群的高度必不小于 1.

定理 7.7　设 $\mathcal{F}, \mathcal{G}, \mathcal{H}/R$ 是形式群,

$$\mathcal{F} \xrightarrow{\ f\ } \mathcal{G} \xrightarrow{\ h\ } \mathcal{H}$$

是同态, 则

(a) 若 $f'(0) = 0$, 则 $f(T) = f_1(T^p)$, 对某个 $f_1(T) \in R[[T]]$;

(b) 若 $f(T) = g(T^{p^h})$, $h = ht(f)$, 则 $g'(0) \neq 0$;

(c) $ht(h \circ f) = ht(f) + ht(h)$.

证明　(a) 令 $\omega_{\mathcal{F}}$ 和 $\omega_{\mathcal{G}}$ 是正规不变微分, 则因 $f'(0) = 0$, 故

$$0 = f'(0)\omega_{\mathcal{F}}(T) = \omega_{\mathcal{F}}\big(f(T)\big) = (1 + \cdots)f'(T)dT \qquad (\text{推论 } 7.1),$$

$\Longrightarrow f'(T) = 0$, 故 $f(T) = f_1(T^p)$.

(b) 记 $q = p^h$, 如果 $F(X, Y) = \sum a_{ij}X^iY^j$ 是 $\mathcal{F}$ 的形式群律, 则形式群律 $F^{(q)}(X, Y) = \sum a_{ij}^q X^iY^j$ 定义出一个形式群 $\mathcal{F}^{(q)}$. 易知 $\mathcal{F}^{(q)}$ 确为形式群 (因 $\mathrm{ch}(R) = p$), 下证 g 是 $\mathcal{F}^{(q)}$ 到 $\mathcal{G}$ 的同态:

$$\begin{aligned}
g\big(F^{(q)}(X, Y)\big) &= g\big(F(S, T)^q\big) && (\text{令 } S^q = X, T^q = Y)\\
&= f\big(F(S, T)\big) && (f(T) = g(T^q))\\
&= G\big(f(S), f(T)\big) && (f \text{ 是同态})\\
&= G\big(g(S^q), g(T^q)\big) = G\big(g(X), g(Y)\big),
\end{aligned}$$

于是由 (a), 若 $g'(0) = 0$, 则 $g(T) = g_1(T^p)$, 从而 $f(T) = g(T^{p^h}) = g_1(T^{p^{h+1}})$, 与 $h = ht(f)$ 矛盾, 所以 $g'(0) \neq 0$.

(c) 写 $f(t) = f_1\big(T^{p^{ht(f)}}\big)$, $h(T) = h_1\big(T^{p^{ht(h)}}\big)$, 则

$$h \circ f(T) = h_1\big(f_1(T^{p^{ht(f)}})^{p^{ht(h)}}\big) = h_1\big(\widetilde{f}_1(T^{p^{ht(f)+ht(h)}})\big).$$

此处 $\widetilde{f}_1$ 是将 f_1 的系数提升 $p^{ht(h)}$ 次幂得到的, 由 (b) 因 h_1 和 f_1 都有非零线性项, 故 $h_1 \circ \widetilde{f}_1(T)$ 的线性项非零, 从而 $ht(h \circ f) = ht(f) + ht(h)$.

定理 7.8 (a) 设 K 为域, $\mathrm{ch}(K)=p>0$, $E_1, E_2/K$ 为椭圆曲线, $\phi: E_1 \to E_2$ 是定义在 K 上的非零同种, 令 $f: \widehat{E_1} \to \widehat{E_2}$ 是由 ϕ 诱导出的形式群的同态, 则

$$\deg_i(\phi) = p^{ht(f)}.$$

(b) 设 E/K 为椭圆曲线, $\mathrm{ch}(K)=p>0$, 则 $ht(\widehat{E})=1$ 或 2.

证明 (a) 第 1 种情形, ϕ 是 p^r 次 Frobenius 映射, 则 $\deg_i \phi = p^r$, 而 $f(T)=T^{p^r}$, 故 $ht(f)=p^r=\deg_i \phi$.

第 2 种情形, ϕ 是可分的, 设 ω 是 E_2/K 上的不变微分形式, $\omega(T)$ 是形式群 $\widehat{E_2}$ 上对应的不变微分, 因 ϕ 是可分的, $\phi^\star\omega \neq 0$, 故由推论 7.1, 知

$$0 \neq \omega \circ f(T) = f'(0)\omega(T),$$

从而 $f'(0) \neq 0$, 即 $ht(f)=0$.

因为每一个同种都是一个 Frobenius 和一个可分映射之复合, (a) 于是由上面第 1 种和第 2 种情形及定理 7.7(c) 和 $\deg_i(\phi\circ\psi)=\deg_i(\phi)\deg_i(\psi)$ 得出.

(b) 将 (a) 应用到 $\phi=[p]$ 可得: 因 $\deg([p])=p^2$, 故 $\deg_i([p])=p$ 或 p^2, 证毕.

第八章　局部域上的椭圆曲线

在本节，我们设 K 是完备局部域，其离散赋值为 v, $R=\{x\in K|v(x)\geqslant 0\}$ 是其整数环，$R^*=\{x\in K|v(x)=0\}$, $\mathcal{M}=\{x\in K|v(x)>0\}$ 是极大理想，$\mathcal{M}=\pi R$, π 是 R 的一致化子，$k=R/\mathcal{M}$ 是剩余类域，且总设 $v(\pi)=1$, $v(0)=\infty$.

§8.1　极小 Weierstrass 方程

设 $E/K: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6$ 是一个 Weierstrass 方程，如果做变量替换 $(x,y)\mapsto(u^{-2}x,u^{-3}y)$, 则 $a_i\mapsto u^ia_i$, 若选取 u, 使得 u 被 π 的大幂次除尽，则可以找到一个 Weierstrass 方程，其所有系数 $a_i\in R$, 从而其判别式 Δ 满足 $v(\Delta)\geqslant 0$. 由于 v 是离散的，我们找一个方程使 $v(\Delta)$ 最小.

定义 8.1　设 E/K 是椭圆曲线，如上的 Weierstrass 方程称为一个极小方程，如果 $a_i\in R$ 且 $v(\Delta)$ 极小，而此时的 $v(\Delta)$ 称为 E 在 v 处的极小判别式赋值.

如何判定一个 Weierstrass 方程是否极小? 因 $a_i\in R\Longrightarrow\Delta\in R$, 若方程不是极小的，则存在一个坐标变换给出一个新方程，其判别式 $\Delta'=u'^{12}\Delta$, 故 $v(\Delta)$ 只能被 12 的倍数改变，故有

$$\text{若 } a_i\in R,\ \text{且 } v(\Delta)<12,\ \text{则方程是极小的.}$$

类似地，因 $c_4'=u^4c_4$, $c_6'=u^6c_6$, 故

$$\text{若 } a_i\in R,\ \text{且 } v(c_4)<4(\text{或 } v(c_6)<6),\ \text{则方程是极小的.}$$

反之，若 $\mathrm{ch}(k)\neq 2,3$, 则可证明逆也成立：即极小方程必有 $v(\Delta)<12$ 或 $v(c_4)<4$.

例 8.1　设 p 为素数，

$$E/\mathbb{Q}_p: y^2+xy+y=x^3+x^2+22x-9,$$

$\Delta=-2^{15}5^2$, $c_4=-5\cdot 211$, 于是由上可知对任意素数 p, 这是一个 Weierstrass 极小方程.

定理 8.1　(a) 每一个椭圆曲线 E/K 有极小方程;

(b) 一个极小方程在如下的坐标变换的意义下是惟一的：

$$x=u^2x'+r,\quad y=u^3y'+u^2sx'+t,\quad u\in R^*, r,s,t\in R;$$

(c) 伴随到极小方程的不变微分

$$\omega = dx/(2y + a_1x + a_3)$$

在相差一个 R^* 中倍数的意义下是惟一的；

(d) 反之，若始于任意 $a_i \in R$ 的 Weierstrass 方程，则任何用来产生极小方程的变换

$$x = u^2x' + r, \quad y = u^3y' + u^2sx' + t$$

必满足 $u, r, s, t \in R$.

证明 (a) 由前面的讨论，总可以找到 E/K 的 Weierstrass 方程，使得 $a_i \in R$，于是由赋值的离散性，知存在最小的 $v(\Delta)$.

(b) 由于 E/K 的任意 Weierstrass 方程在方程 (3.11) 所给出的坐标变换的意义下是惟一的，其中 $u \in K^*, r, s, t \in K$. 现在设所给的方程和经过变换方程 (3.11) 得到的新方程都是极小的，于是有 $v(\Delta) = v(\Delta')$，但是 $\Delta = u^{12}\Delta'$，因此 $v(u) = 0$，故 $u \in R^*$. 再从方程 (3.12) 中关于 b_6(或 b_8) 的变换公式，知 $4r^3 \in R$(或 $3r^4 \in R$)，因此 $r \in R$. 而 a_2 和 a_6 的变换公式分别给出 $s \in R$ 和 $t \in R$.

(c) 因为 $\omega' = u\omega$，于是 (b) 给出 (c).

(d) 因为 $u^{12}\Delta' = \Delta$ 并且 $v(\Delta') \leqslant v(\Delta)$(因新方程是极小的)，可见 $v(u) \geqslant 0$，从而 $u \in R$. 现在重复 (b) 中的证明过程就知道 $r, s, t \in R$.

§8.2 约化映射及其性质

记自然的约化映射 $R \to R/\mathcal{M} = R/\pi R = k:\ t \mapsto \widetilde{t}$. 设已经选取了一个极小方程 $E/K:\ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$. 于是有 $a_i \in R$，将 a_i 约化，得出 k 上的一条曲线

$$\widetilde{E}: \quad y^2 + \widetilde{a_1}xy + \widetilde{a_3}y = x^3 + \widetilde{a_2}x + \widetilde{a_6},$$

则曲线 $\widetilde{E}/k$ 称为 E 模 π 的约化. 因我们始于极小方程，由定理 8.1(b) 知 $\widetilde{E}$ 在 k 上 Weierstrass 方程的标准坐标变换的意义下是惟一的.

现设 $P \in E(K)$，我们总能选取齐次坐标 $P = [x_0, y_0, z_0]$，使得 $x_0, y_0, z_0 \in R$ 且至少有一个属于 R^*，则约化后的点 $\widetilde{P} = [\widetilde{x_0}, \widetilde{y_0}, \widetilde{z_0}] \in \widetilde{E}(k)$，于是得出一个约化映射

$$\begin{aligned} \varphi: \quad & E(K) \longrightarrow \widetilde{E}(k) \\ & P \ \longmapsto \widetilde{P} \end{aligned}$$

(更一般地，我们可以类似地定义约化映射

$$\psi: \quad \mathbb{P}^n(K) \longrightarrow \mathbb{P}(k),$$

而上面的映射就是 ψ 在 $E(K)$ 上的限制).

注意 $\widetilde{E}/k$ 也许是奇异的, 但无论如何, 其非奇异点的集合 $\widetilde{E}_{ns}(k)$ 构成一个群, 定义 $E(K)$ 的一个子集如下:

$$E_0(K) = \{P \in E(K) | \widetilde{P} \in \widetilde{E}_{ns}(k)\},$$
$$E_1(K) = \{P \in E(K) | \widetilde{P} = \widetilde{O}\},$$

即 $E_0(K)$ 是具有非奇异约化的点集, 而 $E_1(K)$ 是约化映射的核.

定理 8.2　*存在一个正合列(Abel 群)*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \widetilde{E}_{ns}(k) \longrightarrow 0,$$

其中右端映射是约化映射.

证明　注意 $E(K)$ 和 $\widetilde{E}_{ns}(k)$ 的群运算是通过 $\mathbb{P}^2$ 中的直线与相应的椭圆曲线的交定义的. 因为约化映射 $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$ 将直线变为直线, 故 $E_0(K)$ 是一个群, 而 $E_0(K) \longrightarrow \widetilde{E}_{ns}(k)$ 是同态. 而左边的正合性是 $E_1(K)$ 的定义. 下证约化是满的: 令

$$f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

是 E/K 的极小方程, $\widetilde{f}(x,y)$ 是 $f(x,y)$ 的约化, $\widetilde{P} = (\alpha,\beta) \in \widetilde{E}_{ns}(k)$ 为任意点, 因 $\widetilde{P}$ 为非奇异点, 故

$$\frac{\partial \widetilde{f}}{\partial x}(\widetilde{P}) \neq 0 \quad 或 \quad \frac{\partial \widetilde{f}}{\partial y}(\widetilde{P}) \neq 0,$$

不妨设为前者, 选取任意 $y_0 \in R$, 使得 $\widetilde{y_0} = \beta$, 方程 $f(x,y_0) = 0$, 该方程的模 π 约化具有一个单根 α (因为 $\partial\widetilde{f}/\partial x(\alpha,\widetilde{y_0}) = \partial\widetilde{f}/\partial x(\alpha,\beta) \neq 0$), 因此由 Hensel 引理, 根 α 能够提升至一个 $x_0 \in R$, 使得 $\widetilde{x_0} = \alpha$ 且 $f(x_0,y_0) = 0$, 于是点 $P = (x_0,y_0) \in E_0(K)$ 约化到 $\widetilde{P}$, 证毕.

定理 8.3　*设 E/K 由极小方程给定, $\widehat{E}/R$ 是伴随到 E 的形式群, $w(z) \in R[[z]]$ 是 §7.1 中引进的幂级数 (7.3), 则映射*

$$\begin{aligned} \widehat{E}(\mathcal{M}) &\longrightarrow E_1(K) \\ z \quad &\longmapsto \left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) \end{aligned}$$

是同构 (其中我们认为 $z = 0$ 对应到无穷远点 $\mathcal{O}$).

证明　由 §7.1 中的内容, 知道点 $\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right)$ 如果考虑作幂级数对, 是满足 E 的 Weierstrass 方程的, 因 $w(z) = z^3(a + \cdots) \in R[[z]]$, 故 $w(z)$ 收敛 ($\forall z \in \mathcal{M}$), 从而

$$\left(\frac{z}{w(z)}, -\frac{1}{w(z)}\right) \in E(K), \quad \forall z \in \mathcal{M},$$

并且因为 $v\left(-\frac{1}{w(z)}\right)=-3v(z)$, 可见它是属于 $E_1(K)$ 的, 从而有映射

$$\begin{aligned}\phi:\quad \widehat{E}(\mathcal{M}) &\longrightarrow E_1(K)\\ z\quad &\longmapsto \big(z/w(z),-1/w(z)\big).\end{aligned}$$

更进一步, 在导出 $\widehat{E}$ 上的群运算时, 我们正是用的 E 上的群运算 (在 (z,w) 平面上的), 然后由 $w(z)$ 代替 w, 故 ϕ 是一个群同态, 又 $w(z)=0$ 当且仅当 $z=0$, 故 ϕ 是单射. 下证 ϕ 是满的. 设 $(x,y)\in E_1(K)$, 因 (x,y) 模 π 约化到 $\widetilde{E}(k)$ 上的无穷远点, 我们看到 $v(x)<0$ 且 $v(y)<0$(比较极小方程两边的赋值即可得出这结果). 又由方程 $y^2+\cdots=x^3+\cdots$, 必有 $3v(x)=2v(y)=-6r$(对某个正整数 $r\geqslant 1$), 从而 $x/y\in\mathcal{M}$, 于是映射

$$E_1(K)\longrightarrow \widehat{E}(\mathcal{M})$$

$$(x,y)\longmapsto -x/y$$

是合理定义的, 且因 $\widehat{E}(\mathcal{M})$ 上群运算是由 E 上群运算所定义的, 它是一个同态, 且显然为单同态, 故有 2 个单射

$$\widehat{E}(\mathcal{M})\longrightarrow E_1(K)\longrightarrow \widehat{E}(\mathcal{M}),$$

其复合是恒等映射, 故它们是同构的.

§8.3 有限阶点

下面讨论 E/K 上的有限阶点.

定理 8.4 设 E/K 是椭圆曲线, $m\geqslant 1$ 与 $\mathrm{ch}(k)$ 互素, 则

(a) 子群 $E_1(K)$ 没有 m 阶点;

(b) 若约化曲线 $\widetilde{E}/K$ 非奇异, 则约化映射

$$E(K)[m]\longrightarrow \widetilde{E}(k)$$

是单的.

证明 由定理 8.3 知

$$0\longrightarrow E_1(K)\longrightarrow E_0(K)\longrightarrow \widetilde{E}_{ns}(k)\longrightarrow 0$$

正合, 但 $E_1(K)\simeq\widehat{E}(\mathcal{M})$, $\widehat{E}$ 为伴随到 E 的形式群, 从关于形式群的一般结果, 知道 $\widehat{E}(\mathcal{M})$ 没有 m 阶点. 这就证明了 (a). 现若 $\widetilde{E}$ 非奇异, 则 $E_0(K)=E(K)$, $\widetilde{E}_{ns}(k)=\widetilde{E}(k)$, 从而 $E(K)$ 中 m 扭元单射到 $\widetilde{E}(k)$ 中, 即 (b), 证毕.

注：定理 8.4 提供了寻找定义在数域上的椭圆曲线的扭点的极快的方法：设 K 是数域 (例如 $K=\mathbb{Q}$), K_v 是 K 在某个离散赋值的完备化, 则 $E(K)\hookrightarrow E(K_v)$ 是嵌入, 于是对几个不同的 v 和 E/K_v 应用定理 8.4, 能够得到关于 $E(K)$ 的很多信息.

例 8.2 设 $E/\mathbb{Q}$ 是椭圆曲线

$$E:\quad y^2=x^3+3,$$

其判别式 $\Delta=-3^5 2^4$, 故 $\widetilde{E}\pmod p$ 是非奇异的, $\forall p\geqslant 5$, 易验证

$$\#\widetilde{E}(\mathbb{F}_5)=6,\quad \#\widetilde{E}(\mathbb{F}_7)=13.$$

从而 $E(\mathbb{Q})$ 没有非平凡的扭元, 特别地, $(1,2)\in E(\mathbb{Q})$ 是无限阶的, 即 $E(\mathbb{Q})$ 为无限集合.

定理 8.5 设 $\mathrm{ch}(K)=0$ 且 $p=\mathrm{ch}(k)>0$, 设 E/K 是一条椭圆曲线,

$$E: y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\qquad a_i\in R.$$

令 $P\in E(K)$ 是一个阶恰为 $m\geqslant 2$ 的点, 则

(a) 若 m 不为 p 的幂次, 则 $x(P),y(P)\in R$;

(b) 若 $m=p^n$, 则

$$\pi^{2r}x(P),\ \pi^{3r}y(P)\in R,\quad r=\left[\frac{v(p)}{p^n-p^{n-1}}\right].$$

证明 若 E 的方程不是极小的, 而 (x',y') 是极小方程的坐标, 则从定理 8.1(d) 知

$$v\big(x(P)\big)\geqslant v\big(x'(P)\big),\quad v\big(y(P)\big)\geqslant v\big(y'(P)\big).$$

可见我们只要对极小方程证明即可.

若 $x(P)\in R$, 则 $y(P)\in R$, 得证, 故设 $v\big(x(P)\big)<0$, 则由 Weierstrass 方程知

$$3v\big(x(P)\big)=2v\big(y(P)\big)=-6s,\qquad 对某个\ s\geqslant 1,$$

且 $P\in E_1(K)$, 从而由定理 8.3 知 $-x(P)/y(P)\in\widehat{E}(\mathcal{M})$, 但由形式群的一般理论, $\widehat{E}(\mathcal{M})$ 的扭元的阶必为 p 的幂, 这就证明了 (a).

而为证明 (b), 应用定理 7.6: 因 $-x(P)/y(P)$ 在 $\widehat{E}(\mathcal{M})$ 中的阶恰为 p^n, 从定理 7.6, 有

$$s=v\big(-x(P)/y(P)\big)\leqslant v(p)/(p^n-p^{n-1}),$$

因为 $\pi^{2s}x(P)$ 和 $\pi^{3s}y(P) \in R$, 这就证明了 (b).

例 8.3 设 $E/\mathbb{Q}$ 是一椭圆曲线, 其 Weierstrass 方程的系数属于 $\mathbb{Z}$, 设 $P \in E(\mathbb{Q})$ 是阶恰为 m 的点, 通过将 $E(\mathbb{Q})$ 嵌入 $E(\mathbb{Q}_p)$(对各种素数 p), 即可利用定理 8.5 导出 P 的坐标的整性条件: 若 m 不是一个素数的幂次, 则定理 8.5(a) 表明对任意素数 p, 均有 $x(P), y(P) \in \mathbb{Z}_p$, 于是 $x(P), y(P) \in \mathbb{Z}$. 但即使 $m = p^n$(p 为某个素, 它对应到一个正规赋值 v), 有

$$\left[v(p)/(p^n - p^{n-1})\right] = \left[1/(p^n - p^{n-1})\right] = 0.$$

除非 $p = 2, n = 1$, 于是若 $m \geqslant 3$, 则由定理 8.5(b), 知 $x(P), y(P) \in \mathbb{Z}_q$, 对任意素数 $q \in \mathbb{Z}$, 即 $x(P), y(P) \in \mathbb{Z}$, 因而有: 每一个阶为 $m \geqslant 3$ 的扭点必是整点. 这是最好可能的, 正如下例所示:

$$E: \quad y^2 + xy = x^3 + x + 1,$$

上有 2 阶点 $(-1/4, 1/8) \in E(\mathbb{Q})[2]$.

§8.4 坐标赋值有限的点集

最后, 我们给出定义: 设 E/K 是由极小方程给出的椭圆曲线, 定义 $E(K)$ 的子集

$$E_n(K) = \{P \in E(K) | v\big(x(P)\big) \leqslant -2n\} \bigcup \{\mathcal{O}\}, \quad n \geqslant 0.$$

则有

定理 8.6 (a) $E_n(K)\big(< E(K)\big)$ *是* $E(K)$ *的子群;*

(b) $\forall n \geqslant 1$, *有同构*

$$E_n(K)/E_{n+1}(K) \simeq k^+ \quad (k^+\text{表示只看 } k \text{ 中加法而成的群}).$$

证明 在 (z, w) 平面上, $E_n(K)$ 中的点可描述为 $v\big(w(P)\big) \geqslant 3n$. 事实上, 由于 $y^2 + \cdots = x^3 + \cdots$, 可知 $3v\big(x(P)\big) = 2v\big(y(P)\big) = -6s, \quad s \geqslant n$, 从而由 $z = -x/y, w = -1/y$ 知, $v\big(w(P)\big) \geqslant 3n, v\big(z(P)\big) \geqslant n$.

(a) $n = 0, 1$ 时是显然的 (定理 8.2). 下面不妨设 $n > 1$, 则由定理 8.3 知

$$\begin{array}{ccccc} \widehat{E}(\mathcal{M}) & \longrightarrow & E_1(K) & \longrightarrow & \widehat{E}(\mathcal{M}) \\ z & \longmapsto & \left(\dfrac{z}{w(z)}, -\dfrac{1}{w(z)}\right), (x, y) & \longmapsto & -x/y \end{array}$$

是同构. 于是由刚才的说明知道

$$P=(x,y)\in E_n(K) \iff v\big(x(P)\big)\leqslant -2n \iff v\big(w(P)\big)\geqslant 3n$$
$$\iff v\big(-x/y\big)\geqslant 3n \iff v\big(z(P)\big)\geqslant n.$$

可见

$$\begin{aligned}\widehat{E}(\mathcal{M}^n) &\longrightarrow E_n(K)\\ z &\longmapsto \left(\frac{z}{w(z)},-\frac{1}{w(z)}\right)\end{aligned}$$

是一个同构, 从而 $E_n(K)$ 是一个群, 它同构于 $\widehat{E}(\mathcal{M}^n)$, $E_n(K)<E(K)$, 由定理 7.3 知

$$E_n(K)/E_{n+1}(K)\simeq \widehat{E}(\mathcal{M}^n)/\widehat{E}(\mathcal{M}^{n+1})\simeq \mathcal{M}^n/\mathcal{M}^{n+1}\simeq k^+.$$

证毕.

定理 8.7 设 E/K 是由极小方程给出的椭圆曲线, 则 $E_n(K)$ 是 $E(K)$ 的子群, 且映射

$$\begin{array}{ccccc} E_n(K) & \longrightarrow & \pi^n R=\mathcal{M}^n & \longrightarrow & \mathcal{M}^n/\mathcal{M}^{2n}\\ (z,w) & \longmapsto & z & \longmapsto & z \pmod{\mathcal{M}^{2n}}\end{array}$$

是一个群同态, 其核在 $E_{2n}(K)$ 中, 它诱导出一个单同态

$$E_n(K)/E_{2n}(K)\longrightarrow \mathcal{M}^n/\mathcal{M}^{2n},\quad \forall n\geqslant 1,$$

且若 $a_1=0$, 则还有单射

$$E_n(K)/E_{3n}(K)\longrightarrow \mathcal{M}^n/\mathcal{M}^{3n}.$$

证明 注意到

$$z_1\bigoplus_{\widehat{E}} z_2=z_1+z_2-a_1z_1z_2-a_2(z_1^2z_2+z_1z_2^2)+\cdots.$$

可见, 若 $z_1,z_2\in\mathcal{M}^n$, 则

$$z_1\bigoplus_{\widehat{E}} z_2\equiv z_1+z_2 \pmod{\mathcal{M}^{2n}},$$

且若 $a_1=0$, 则

$$z_1\bigoplus_{\widehat{E}} z_2\equiv z_1+z_2 \pmod{\mathcal{M}^{3n}}.$$

证毕.

定理 8.8 设 E/K 是椭圆曲线, $\mathrm{ch}(K)=0, \mathrm{ch}(k)=p>2$, 且离散赋值 $v(p)=1$, 则有

$$E(K)_{\mathrm{tors}} \bigcap E_1(K) = \{\mathcal{O}\}.$$

证明 由定理 8.5 知在定理 8.8 的假设条件下, 有 $\forall P \in E(K)_{\mathrm{tors}}$, 则

$$x(P), y(P) \in R \Longrightarrow v\big(x(P)\big) \geqslant 0,$$

但由于

$$E_1(K) = \big\{P \in E(K) | v\big(x(P)\big) \leqslant -2\big\} \bigcup \{\mathcal{O}\},$$

$\Longrightarrow E(K)_{\mathrm{tors}} \bigcap E_1(K) = \{\mathcal{O}\}$, 证毕.

第九章　Satoh 方法的理论基础

§9.1　引　　论

设 p 是素数, $N \in \mathbb{N}$, $q := p^N$, 记 $\mathbb{F}_q$ 是 q 个元素的有限域. 设 E 是 $\mathbb{F}_q$ 上的一条椭圆曲线, 我们的目的是计算 E 上的 $\mathbb{F}_q$ 有理点的个数 (假设 p 比较小, 而 N 较大).

我们知道, 对于 p 较大的域, 有所谓的 SEA 算法: 其主要思想是计算 $\mathrm{tr}(Fr_q) \pmod{l}$, 此处 l 是一些小素数, 而 Fr_q 是 q 次 Frobenius 映射, 由 Hasse 不等式, 有

$$\left|\mathrm{tr}Fr_q\right| \leqslant 2\sqrt{q},$$

因此, 利用中国剩余定理, 只要求出足够多的 l, 使得 $\prod l > 4\sqrt{p}$, 且计算出 $\mathrm{tr}(Fr_q) \pmod{l}$, 则可定出 $\mathrm{tr}\,Fr_q$ 的正确值, 从而计算出点数等于 $q+1-\mathrm{tr}Fr_q$.

记 $\mathcal{M} \in \mathbb{R}$, 使得两个 n-bits 的整数之积在 $O(n^{\mathcal{M}})$ 个比特运算内完成, 则 SEA 算法的时间复杂度是 $O\big((\log q)^{2\mathcal{M}+2}\big)$. 在具体的算法中, 最耗时间的部分是对于大约 $O\big(\log q\big)$ 个 l, 计算 Frobenius 的作用. 因此, 要找出一个更快速的算法, 关键在于如何避免使用 E 的 Frobenius 自同态.

在 Satoh 给出的方法中, 最本质之处就是避免了 Frobenius 的作用, 其方法对于小的素数 p 和大的 N 是极为有效的. 整个 Satoh 算法的时间复杂度是 $O\big(N^{2\mathcal{M}+1}\big)$ 个比特运算, 此处 O 常数取决于 p.

设 $E/\mathbb{F}_q$ 是一条椭圆曲线, 下面假定 $j(E) \notin \mathbb{F}_{p^2}$ (特别地, 这意味着 E 是 ordinary 的), 替代用 Frobenius 来计算 $\mathrm{tr}\,Fr_q$, 我们将应用其对偶 (称为 Verschiebung) V_p.

对于一条 ordinary 的椭圆曲线 $E/\mathbb{F}_q$, 记其典范提升为 $E^{\uparrow}$, 它是定义在 $\mathbb{Q}_p$ 的某个非分歧扩张上的一条椭圆曲线. E 的典范提升由下面两个性质所刻画: $E^{\uparrow} \pmod{p}$ 的约化是 E, 且 $\mathrm{End}(E) \simeq \mathrm{End}(E^{\uparrow})$(作为一个环). Deuring 的一个经典结果是 $E^{\uparrow}$ 存在, 且在同构意义下是惟一的. 如果 E 和 E' 是 $\mathbb{F}_q$ 上 ordinary 的椭圆曲线, 则

$$\mathrm{Hom}(E, E') \simeq \mathrm{Hom}(E^{\uparrow}, E'^{\uparrow}).$$

令 $E^{(i)} := Fr_p^i E$, 因为 E 是 ordinary 的, 所有的椭圆曲线 $E^{(i)}\,(i=0,1,\cdots,N-1)$ 也是 ordinary 的, 且 $V_p : E^{(i)} \to E^{(i-1)}$ 是可分的. 因此 V_p 被其核所惟一决定. 这意味着能够清晰地提升 V_p 到 $V_p^{\uparrow} : E^{(i)\uparrow} \to E^{(i-1)\uparrow}$, 方法是通过提升 V_p 的核 $E[p]$.

通过观察 $V_p^{\uparrow N}: E^{\uparrow} \to E^{\uparrow}$ 在 $E^{\uparrow}$ 的形式群上的作用, 可以得到 $V_p^{\uparrow N}$ 的迹, 该迹也等于 Fr_q 的迹 (见图 9.1).

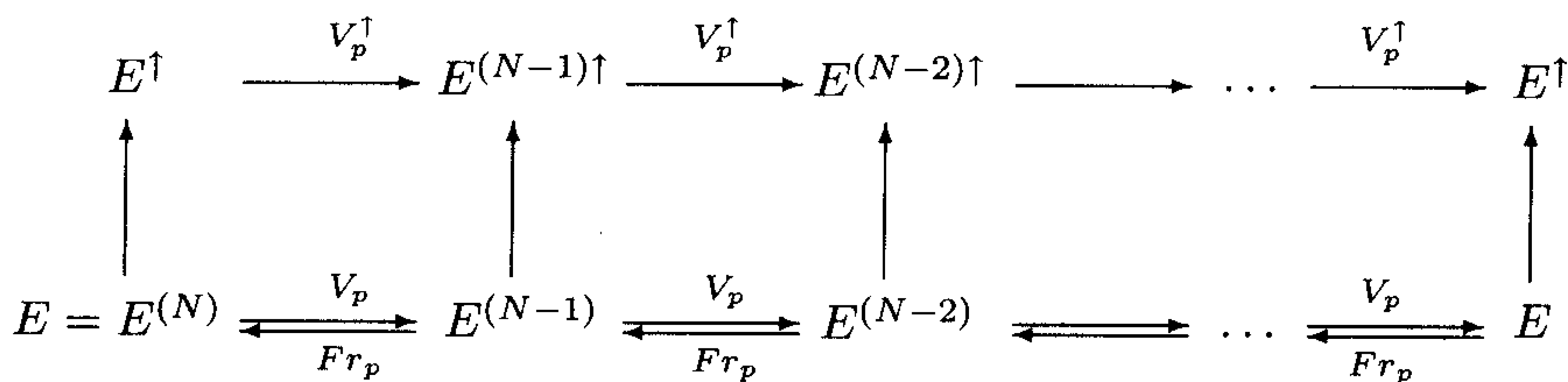


图 9.1

记号: 除非特别申明, 总假设 $p \geqslant 5$ 是一个素数, $N \in \mathbb{N}$, $q := p^N$. 选择且固定一个次数 N 的非分歧扩张 $K/\mathbb{Q}_p$, 记 K 的赋值环为 R, 因 $K/\mathbb{Q}_p$ 非分歧, p 在 K 中仍为素数, 且 R 的剩余类域是 $\mathbb{F}_q$. 记 K 的极大非分歧扩张及其赋值环为 K^{ur} 和 R^{ur}. 一般来说, $\mathcal{O}$ 总是记椭圆曲线上的无穷远点, π 是 $\pmod p$ 的约化映射, $\mathrm{Isog}(E_1, E_2)$ 记从 E_1 到 E_2 的 isogenies 的全体. p 次模多项式记为 Φ_p, 记 X 坐标函数和 Y 坐标函数为 ξ 和 η.

§9.2 多项式的因子的提升

在本节中, 我们给出一个提升某类多项式的一个因子的方法, 更确切地说, 设 $U \in R[X]$ 且有 $\pi(U)$ 的一个因子 $f \in \mathbb{F}_q[X]$, 我们想提升 f 到 U 的一个因子 g(即使 $\pi(U)$ 是一个不可约多项式的幂次). 这是 Hensel 引理的变种, 但要考虑计算复杂度. 我们的算法是基于 Zassenhaus 的 2 次提升.

设 $f, g \in R[X]$, $\big(\pi(f), \pi(g)\big) = 1$, 则对于每个 $u \in \mathbb{N}$, 存在 A_u, $B_u \in R[X]$ 满足 $A_u f + B_u g = 1 \pmod{p^u}$. 更进一步, 若 f 是首 1 的, 我们能在 $O\big((\deg f + \deg g)^2\big)$ 个 R/p^uR 上算术运算内构造 A_u 和 B_u, 使得 $\deg B_u < \deg f$.

引理 9.1 设 p 为奇素数, $U \in R[X]$, 令 $t := \mathrm{ord}_p \partial U$, 此处 $\partial = \frac{d}{dX}$. 设 $f \in R[X]$ 是满足下述条件的多项式:

(i) f 首 1;

(ii) $\pi(f)$ 无平方因子;

(iii) $\pi(f)$ 与 $\pi(p^{-t}\partial U)$ 互素;

(iv) 存在 $Q_0 \in R[X]$, $u \in \mathbb{N}$, 使得 $\mathrm{ord}_p\big(U - fQ_0\big) \geqslant u + t$.

令 $v := 2u + \min(t, u)$, 则有下述的:

(a) 假定存在 $g, Q_1 \in R[X]$, 满足 $g \equiv f \pmod p$ 且 $\mathrm{ord}_p\big(U - gQ_1\big) \geqslant v$, 则对所有 $h \in R[X]$, 使得 $h \equiv g \pmod{p^{2u}}$, 存在 $Q_2 \in R[X]$(取决于 h) 满足 $\mathrm{ord}_p\big(U - hQ_2\big) \geqslant v$;

(b) 存在 $Q_3 \in R[X]$ 及首 1 多项式 $g \in R[X]$, 满足

$$\operatorname{ord}_p(U - gQ_3) \geqslant v,$$

且 $g \equiv f \pmod{p^u}$(注意必定 $\pi(g) = \pi(f)$ 且 $\deg g = \deg f$). 我们能用 $R/p^{2u}R$ 上 $O\big((\deg f + \deg g)^2\big)$ 个算术运算构造 g.

证明　(a) 置 $\delta = p^{-2u}(h - g) \in R[X]$, 因 $g \equiv f \pmod p$, 约化 $\pi(g)$ 也是无平方因子的, 由上面的注记, 存在多项式 $A, B \in R[X]$, 使得

$$A\partial g + Bg \equiv \delta \pmod{p^{v-2u}}.$$

但另一方面, $\operatorname{ord}_p(U - gQ_1) \geqslant v$ 表明 $U \equiv gQ_1 \pmod{p^v}$, 从而用 $X + p^{2u}A(X)$ 替代 X, 得出

$$U\big(X + p^{2u}A(X)\big) \equiv g\big(X + p^{2u}A(X)\big)Q_4(X) \pmod{p^v}, \tag{9.1}$$

其中 $Q_4(X) := Q_1\big(X + p^{2u}A(X)\big)$, 展开上式左边, 得

$$U(X) + p^{2u}A(X)\partial U(X) \equiv U(X) \pmod{p^v}.$$

令 $Q_5(X) := \big(1 - p^{2u}B(X)\big)Q_4(X)$, 注意到

$$\big(1 + p^{2u}B\big)\big(1 - p^{2u}B\big) \equiv 1 \pmod{p^v},$$

故 (9.1) 式右端 $\bmod p^v$ 等于 (将 $g\big(X + p^{2u}A(X)\big)$ 展开):

$$\begin{aligned}
&\big(g(X) + p^{2u}A(X)\partial g(X)\big)\big(1 + p^{2u}B(X)\big)Q_5(X) \\
\equiv&\big(g(X) + p^{2u}(A(X)\partial g(X) + g(X)B(X))\big)Q_5(X) \pmod{p^v} \\
\equiv&h(X)Q_5(X) \pmod{p^v},
\end{aligned}$$

因此可以取 $Q_5(X)$ 作为要找的 Q_2.

(b) 令 Y 为一不定元, 置 $r_0 := p^{-u-t}\big(U - fQ_0\big)$, $r_1 := p^{-t}\partial U$, 如果必要, 通过变换 Q_0, 总可假定 $\deg_X r_0(X) < \deg_X f(X)$, 即可以假定 $r_0 = p^{-u-t}\big(U \pmod f\big)$, 于是 Taylor 展开

$$U\big(X + p^u Y\big) = U(X) + p^u Y\partial U(X) + \frac{p^{2u}}{2}Y^2\partial^2 U(X) + \sum_{i=3}^{\infty}\frac{p^{iu}}{i!}Y^i\partial^i U(X).$$

因总设 $p \geqslant 5$, 故 $\operatorname{ord}_p(\frac{p^{2u}}{2}\partial^2 U(X)) \geqslant 2u + t$, 而对于上式右端最后一项, $\frac{\partial^i U(X)}{i!} \in$

$R[X]$ 表明 $\operatorname{ord}_p\left(\frac{p^{iu}}{i!}y^i\partial^i U(X)\right) \geqslant 3u$, 从而有

$$\begin{aligned} U\big(X+p^uY\big) &\equiv U(X)+p^uY\partial U(X) \pmod{p^v} \\ &\equiv p^{u+t}r_0(X)+f(X)Q_0(X)+p^{u+t}r_1(X) \pmod{p^v} \\ &\equiv f(X)Q_0(X)+p^{u+t}\big(r_0(X)+Yr_1(X)\big) \pmod{p^v}. \end{aligned}$$

由条件 (iii), 存在 $A(X),\ B(X) \in R[X]$ 满足

$$A(X)f(X)+r_1(X)B(X) \equiv r_0(X) \pmod{p^u},$$

且 $\deg_X B(X) < \deg_X f(X)$, 因此

$$U\big(X+p^uY\big) \equiv f(X)Q_0(X)+p^{u+t}\big(A(X)f(X)+r_1(X)(Y+B(X))\big) \pmod{p^v}. \tag{9.2}$$

在此式中以 $X+p^uB(X)$ 替代 X, 以 $-B(X)$ 替代 Y, 则有

$$U(X) \equiv f\big(X+p^uB(X)\big)Q_6(X) \pmod{p^v}, \tag{9.3}$$

其中 $Q_6(X) := Q_0\big(X+p^uB(X)\big)+p^{u+t}A\big(X+p^uB(X)\big)$, 将 f 按 Taylor 展开, 有

$$f\big(X+p^uB(X)\big) \equiv f(X)+p^uB(X)\partial f(X)+\frac{p^{2u}}{2}B(X)^2\partial^2 f(X) \pmod{p^{3u}}. \tag{9.4}$$

联合 (9.3) 和 (9.4) 式, 应用结论 (a), 可知存在 $Q_7 \in R[X]$, 使得

$$U(X) \equiv \big(f(X)+p^uB(X)\partial f(X)\big)Q_7(X) \pmod{p^v}.$$

定义 $Q_8, r_2 \in K[X]$ 如下: $B\partial f = Q_8 f + r_2, \deg r_2 < \deg f$, 则 $Q_8,\ r_2$ 属于 $R[X]$(由 (i)), 因

$$\big(1-p^uQ_8+p^{2u}Q_8^2\big)\big(1+p^uQ_8\big) \equiv 1 \pmod{p^{3u}},$$

故有

$$\begin{aligned} U(X) \equiv& \big(f(X)+p^u\big(Q_8(X)f(X)+r_2(X)\big)\big) \\ &\times\big(1-p^uQ_8(X)+p^{2u}Q_8^2(X)\big)\big(1+p^uQ_8\big)Q_7 \\ \equiv& \big(f+p^ur_2+p^{2u}Q_9\big)Q_{10} \pmod{p^v}, \end{aligned} \tag{9.5}$$

其中 $Q_9 := Q_8^2f-Q_8B\partial f = -Q_8r_2$, $Q_{10} := \big(1+p^uQ_8\big)Q_7$. 令 $g := f+p^ur_2$, 则 g 是首 1 的, 且 $g \equiv f \pmod{p^u}$, 现在对 (9.5) 式应用结论 (a)($Q_1 \leftrightarrow Q_{10}$, $f+p^ur_2+p^{2u}Q_9 \leftrightarrow g$, $h \leftrightarrow f+p^ur_2 = g$), 知存在 Q_3, 使得 (b) 成立. 关于计算复杂度的断言是显然的, 证毕.

引理 9.2 设 p 为素数, $U \in R[X]$, $\{a_n\}_{n=1}^{\infty}$ $(a_n \in \mathbb{N})$ 为严格递增序列, 设 $\{h_n \in R[X]\}_{n=1}^{\infty}$ 是首 1 多项式的序列, 满足

(i) $h_{n+1} \equiv h_n \pmod{p^{a_n}}$;

(ii) 对每个 n, 存在 $S_n \in R[X]$, 使得 $\mathrm{ord}_p\big(U - h_nS_n\big) \geqslant a_n$;

(iii) $\pi(h_1)$ 是无平方因子的.

则 $h := \lim\limits_{n\to\infty} h_n \in R[X]$ 存在, 且 $\deg h = \deg h_n$ (对所有 n), h 的所有零点均位于 R^{ur} 中且它们是 U 的零点, 特别地, h 是 U 的一个因子.

证明 因 $R[[X]]$ 关于 p-adic 赋值是完备的, 由条件 (i) 知 $\lim_{n\to\infty} h_n$ 在 $R[[X]]$ 中存在. 更进一步, 条件 (i) 结合 h_n 是首 1 的, 意味着 $\deg h_n = \deg h_1\,(\forall\, n)$, 因此 h 事实上属于 $R[X]$, 并且 $\deg h = \deg h_n\,(\forall n)$. 现设 θ 是 $h(X) = 0$ 之一根. 因为 $\pi(h) = \pi(h_1)$ 是无平方因子的, $\theta \in R^{ur}$, 余下的是要证明 $U(\theta) = 0$. 但是

$$U = \big(U - h_nS_n\big) + (h_n - h)S_n + hS_n,$$

可见 $\mathrm{ord}_pU(\theta) \geqslant a_n$ 对任意 n 成立, 故 $U(\theta) = 0$, 证毕.

§9.3 典范提升的构造

设 E 是一条椭圆曲线 (在 $\mathbb{F}_q$ 上定义的), 且 $j(E) \notin \mathbb{F}_{p^2}$, 在本节中, 我们给出一个构造充分接近 E 的典范提升 (p-adic 意义下) 的椭圆曲线的算法. 应用这些结果, 我们提升 $E[p]$ 到 E 的典范提升的 R^{ur} 值点.

设 k 是一个域, S 是 k 的代数闭包的子环, 对于椭圆曲线

$$E/k: \quad Y^2 = X^3 + AX + B,$$

令

$$E(S) := \{(x, y) \in S^2 | y^2 = x^3 + Ax + B\} \cup \{\mathcal{O}\}.$$

注意, 当 S 不是一个域时, $E(S)$ 一般不是一个群. 应用 $\tau(X, Y) = -X/Y$ 作为在 $\mathcal{O}$ 点的局部参数, 记 $E[n]$ 为 n-torsion 点的群. 对于 $\wp \subset E$, 记 $k(\wp)$ 是由所有属于 $\wp - \{\mathcal{O}\}$ 的点之坐标生成的 k 的扩域.

设 $\psi_p(X, \alpha, \beta) \in \mathbb{Z}[X, \alpha, \beta]$ 是 p 次除子多项式, 此处 α 和 β 是不定元, 因此 $P := (x, y) \in E - \{\mathcal{O}\}$ 是 $E[p]$ 中点当且仅当 $\psi_p(x, A, B) = 0$, 并且存在 φ_p 和 $\Omega_p \in \mathbb{Z}[X, \alpha, \beta]$, 使得

$$pP = \left(\frac{\varphi_p(x, A, B)}{\psi_p(x, A, B)^2}, y\frac{\Omega_p(x, A, B)}{\psi_p(x, A, B)^3}\right), \quad \forall\, P = (x, y) \in E \setminus E[p],$$

并且多项式 $\psi_p(X,A,B)$ 与 $\varphi_p(X,A,B)$ 是互素的. 除子多项式的基本性质前面已经讨论过 (见 §2.4), 注意当 p 为奇数时, $\Omega_p = y^{-1}\omega_p$, 此处 $\omega_m = \frac{1}{4y}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)$(见定理 2.11).

现在设

$$E/\mathbb{F}_q: \quad Y^2 = X^3 + AX + B$$

是 ordinary 的椭圆曲线, 且 $AB \neq 0$, 而令

$$\widetilde{E}: \quad Y^2 = X^3 + \widetilde{A}X + \widetilde{B},$$

是它到 K 上的提升, 注意以下事实: $\widetilde{E}(R^{ur})$ 是一个群.

定理 9.1 设 E 和 $\widetilde{E}$ 如上, 则下面的条件(i)$\sim$ (iv)是等价的:

(i) $\widetilde{E}[p]\bigcap\widetilde{E}(R^{ur}) \neq \{\mathcal{O}\}$;

(ii) 存在 $P \in \widetilde{E}(R^{ur}) - \{\mathcal{O}\}$, 使得 $\tau(pP) \in p^2R^{ur}$;

(iii) 存在 $P = (x,y) \in \widetilde{E}(R^{ur}) - \{\mathcal{O}\}$, 使得 $\psi_p(x,\widetilde{A},\widetilde{B}) \equiv 0 \pmod{p^2}$;

(iv) $j(\widetilde{E}) \equiv j(E^{\uparrow}) \pmod{p^2}$.

证明 (i) $\Longrightarrow$(ii), (iii) 是显然的.

(ii) $\Longrightarrow$ (i): 由假设, 存在 $Q \in \widetilde{E}(K^{ur}) \cap \operatorname{Ker}\pi = \widetilde{E}(K^{ur}) \cap \widetilde{E}_0(K^{ur})$, 使得 $\tau(Q) = \frac{1}{p}\tau(pP) \in pR^{ur}$. 由形式群的有关结果 (见定理 8.3), 知

$$\tau: \quad \operatorname{Ker}\pi\bigcap\widetilde{E}(K^{ur}) \longrightarrow pR^{ur}$$

是一个群同构, 但 $P - Q \in \operatorname{Ker}\pi \cap \widetilde{E}(K^{ur})$ 且

$$\tau\big(p(P-Q)\big) = \tau(pP) - \tau(pQ) = \tau(pP) - p\tau(Q) = \tau(pP) - \tau(pP) = 0,$$

故 $p(P-Q) = 0$, 即 $P - Q \in \widetilde{E}[p] \cap \widetilde{E}(R^{ur})$, 又注意到 $\widetilde{E}_{\text{tors}}(R^{ur}) \cap \operatorname{Ker}\pi = \{\mathcal{O}\}$(见定理 8.8), 故 $P - Q \neq \mathcal{O}$.

(iii)$\Longrightarrow$ (ii): 若 $pP \neq \mathcal{O}$, 则无需再证. 否则, 置 $(x',y') := pP$. 由假设条件 (iii), 知

$$\varphi_p(x,\widetilde{A},\widetilde{B}) \neq 0 \pmod{p}$$

(否则, $\varphi_p(X,A,B) \in \mathbb{F}_q[x]$ 与 $\psi_p(X,A,B) \in \mathbb{F}_q[x]$ 将不互素, 与除子多项式的性质矛盾), 因此

$$\operatorname{ord}_p x' = \operatorname{ord}_p \varphi_p(x,\widetilde{A},\widetilde{B}) - 2\operatorname{ord}_p \psi_p(x,\widetilde{A},\widetilde{B}) \leqslant -4,$$

而 $\operatorname{ord}_p y' = \frac{3}{2}\operatorname{ord}_p x'$, 从而 $\tau(pP) = -x'/y' \equiv 0 \pmod{p^2}$.

(i) $\Longrightarrow$ (iv): 令 $H := \widetilde{E}[p] \cap \widetilde{E}(R^{ur})$, 则 $H \neq \{\mathcal{O}\}$ 是一个群. 且由定理 8.2, 有正合列

$$0 \longrightarrow H \longrightarrow \widetilde{E}[p] \xrightarrow{\pi} E[p] \longrightarrow 0.$$

因为 E 是 ordinary 的, 故 $E[p] \simeq \mathbb{Z}/p\mathbb{Z}$, 又 $\widetilde{E}[p] \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, 可见 H 是一个 p 阶循环群, 再令 $G := \widetilde{E}[p] \cap \operatorname{Ker}\pi$, 再由上述正合列, 可知 G 也是一个 p 阶循环群. 又由于 $\widetilde{E}_{\text{tors}}(R^{ur}) \cap \operatorname{Ker}\pi = \{\mathcal{O}\}$, 从而知, 作为一个群, 有

$$\widetilde{E}[p] = H \oplus G.$$

现考虑域 $K(G)$, 因为 G 是 p 阶循环群, 所以 $G = \langle Q \rangle, \forall Q \in G - \{\mathcal{O}\}$, 从而

$$K(G) = K\big(\xi(Q), \eta(Q)\big), \quad \forall Q \in G - \{\mathcal{O}\},$$

其中 $\xi(Q)$ 和 $\eta(Q)$ 分别表示点 Q 的横坐标和纵坐标. 因为任何其它点 $Q' \in G$ 的坐标均为 $\xi(Q)$ 和 $\eta(Q)$ 的有理函数 (系数在 K 中), 注意到 G 和 H 均定义在 K 上, 所以 $\xi(Q)$ 的共轭元的数目不应超过 $G - \{\mathcal{O}\}$ 中点的 X 坐标的数目, 即不超过 $\frac{p-1}{2}$, 故

$$\big[K(G):K\big] = \big[K(\xi(Q),\eta(Q)) : K(\xi(Q))\big]\big[K(\xi(Q)):K\big] \leqslant 2 \cdot \frac{p-1}{2} = p-1.$$

另一方面, $K(H)/K$ 是非分歧的扩张, 所以 $K\big(\widetilde{E}[p]\big)/K$ 是 tamely 分歧的. 利用 Nakamura 的结果, 这就产生了结果 (iv).

(iv) $\Longrightarrow$ (iii): 首先证明 $E^{\uparrow}[p] \cap E^{\uparrow}(R^{ur}) \neq \{\mathcal{O}\}$. 令 V_p 是 E 的 Verschiebung (即 p 次 Frobenius 的对偶) 且 $V_p^{\uparrow} \in \operatorname{End}(E^{\uparrow})$ 是 V_p 到 $\operatorname{End}(E^{\uparrow})$ 的提升. 因 V_p 是可分的 (这是因为 E 是 ordinary 的), 知 $\pi\big(\operatorname{Ker} V_p^{\uparrow}\big) = \operatorname{Ker} V_p = E[p]$. 这表明

$$\prod_{P \in \left(\operatorname{Ker} V_p^{\uparrow} - \{\mathcal{O}\}\right)/\pm 1} \big(X - \xi(P)\big) \in R[X]$$

的 mod p 约化是无平方因子的. 于是由文献 [11] 中 [Prop. II4.7] 知, 对于 $P \in \operatorname{Ker} V_p^{\uparrow} - \{\mathcal{O}\}$ 有 $\xi(P) \in R^{ur}$, 又由

$$\eta(P)^2 = \xi(P)^3 + A^{\uparrow}\xi(P) + B^{\uparrow}$$

及 $\xi(P), A^{\uparrow}, B^{\uparrow} \in R^{ur}$ 知 $\eta(P)^2 \in R^{ur}$. 下证 $\operatorname{ord}_p\eta(P) = 0$, 若不然, 设 $\operatorname{ord}_p\eta(P) > 0$, 则 $\operatorname{ord}_p\xi(P) = 0$(否则 $\operatorname{ord}_p\xi(P) > 0$, 故 $\operatorname{ord}_p B^{\uparrow} > 0$, 即 $A^{\uparrow}B^{\uparrow} \equiv AB = 0 \pmod p$, 与假设 $AB \neq 0$ 矛盾). 令 $\big(\xi(P), \eta(P)\big)$ 的 mod p 约化是 E 上的点 (α, β), 则 $\beta = 0$, $\alpha^3 + A\alpha + B = 0$, 可见 $(\alpha, 0) \in E[2]$. 另一方面

$$p\big(\xi(P), \eta(P)\big) = \mathcal{O}.$$

mod p 约化, 注意到 p 为奇数, 有

$$\mathcal{O} = p(\alpha, 0) = (\alpha, 0) + (p-1)(\alpha, 0) = (\alpha, 0)$$

(因为 $(p-1)(\alpha,0) = \frac{p-1}{2}(2(\alpha,0)) = \frac{p-1}{2}\cdot\mathcal{O} = \mathcal{O}$), 矛盾. 可见 $\mathrm{ord}_p\eta(P) = 0$.

由 $\eta(P)^2 \in R^{ur}$ 及 $\mathrm{ord}_p\eta(P) = 0$, 可知 $\eta(P) \in R^{ur}$(Hensel 引理), 故 $E^{\uparrow}[p] \cap E^{\uparrow}(R^{ur}) \neq \{\mathcal{O}\}$. 于是 (i) 对 $E^{\uparrow}$ 成立, 从而 (iii) 对 $E^{\uparrow}$ 成立, 设 $Y^2 = X^3 + A^{\uparrow}X + B^{\uparrow}$ 是 $E^{\uparrow}$ 的 Weierstrass 方程, 则 $j(\widetilde{E}) \equiv j(E^{\uparrow}) \pmod{p^2}$ 表明 $\widetilde{A} \equiv u^2 A^{\uparrow} \pmod{p^2}$ 且 $\widetilde{B} \equiv u^3 B^{\uparrow} \pmod{p^2}$, 此处

$$u := \frac{\widetilde{A}B^{\uparrow}}{A^{\uparrow}\widetilde{B}} \in R^* \quad (AB \neq 0, \text{因此}\widetilde{A},\ \widetilde{B},\ A^{\uparrow},\ B^{\uparrow} \in R^*),$$

但这意味着 (iii) 对 $\widetilde{E}$ 成立 (因为 (iii) 仅仅取决于 $\widetilde{A} \pmod{p^2}$ 和 $\widetilde{B} \pmod{p^2}$), 证毕.

下面, 设 Φ_p 是 p 次模多项式.

命题 9.1 设 $m \in \mathbb{N}$, $z_0, \cdots, z_{N-1} \in R$, 使得

(i) $z_i \equiv z_{i+1}^p \pmod{p}$;

(ii) $\pi(z_i) \notin \mathbb{F}_{p^2}$;

(iii) $\Phi_p(z_i, z_{i+1}) \equiv 0 \pmod{p^m}$, 对一切 $0 \leqslant i < N$ 成立.

此处, 我们认为 $z_N = z_0$, 则存在 $\zeta_0, \cdots, \zeta_{N-1} \in R$, 它们在模 p^{2m} 的意义下是惟一的, 且满足 $\forall 0 \leqslant i < N$(同样我们认为 $\zeta_N = \zeta_0$):

(a) $\zeta_i \equiv z_i \pmod{p^m}$;

(b) $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0 \pmod{p^{2m}}$;

更进一步 (一旦 $\Phi_p \pmod{p^{2m}}$ 计算出来), 在 $O(N)$ 个 $R \pmod{p^{2m}}$ 上的算术运算内可得到 $\zeta_i \pmod{p^{2m}}$, $\forall 0 \leqslant i < N$.

证明 回顾模多项式满足下面的 Kronecker 关系:

$$\Phi_p(U, V) \equiv (U^p - V)(U - V^p) \pmod{p},$$

因此, 由 (i) 有

$$\frac{\partial\Phi_p}{\partial U}(z_i, z_{i+1}) \equiv z_{i+1}^{p^2} - z_{i+1} \pmod{p}, \tag{9.6}$$

$$\frac{\partial\Phi_p}{\partial V}(z_i, z_{i+1}) \equiv 0 \pmod{p}. \tag{9.7}$$

定义从 $R^N \to R^N$ 的映射 $\mathcal{F}$:

$$\mathcal{F}\left({}^t(x_0, \cdots, x_{N-1})\right) := {}^t\left(\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \cdots, \Phi_p(x_{N-1}, x_0)\right).$$

令 $z := {}^t(z_0, z_1, \cdots, z_{N-1})$, 对于 $\delta \in R^N$, 由 Taylor 公式知

$$\mathcal{F}(z + p^m\delta) \equiv \mathcal{F}(z) + (D\mathcal{F})(z)p^m\delta \pmod{P^{2m}}, \tag{9.8}$$

其中

$$(D\mathcal{F})(z) := \begin{pmatrix} \frac{\partial\Phi_p}{\partial U}(z_0, z_1) & \frac{\partial\Phi_p}{\partial V}(z_0, z_1) & 0 & \cdots & 0 \\ 0 & \frac{\partial\Phi_p}{\partial U}(z_1, z_2) & \frac{\partial\Phi_p}{\partial V}(z_1, z_2) & \cdots & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \frac{\partial\Phi_p}{\partial V}(z_{N-1}, z_0) & 0 & 0 & \cdots & \frac{\partial\Phi_p}{\partial U}(z_{N-1}, z_0) \end{pmatrix},$$

由 (9.6) 和 (9.7) 式知 $(D\mathcal{F})(z) \pmod p$ 是对角阵, 而由条件 (ii) 知其对角线上的元素是非零的 (因 $\pi(z_i) = z_i \pmod p$, 而 $\pi(z_i) \notin \mathbb{F}_{p^2}$, 故 $z_i^{p^2} \neq z_i \pmod p$), 所以 $\det\big(D\mathcal{F})(z) \in R^*$, 置 $\delta := -p^{-m}(D\mathcal{F})(z)^{-1}\mathcal{F}(z)$, 由 (iii) 知 $\delta \in R^N$. 现在

$${}^t\big(\zeta_0, \cdots, \zeta_{N-1}\big) := z + p^m\delta$$

就满足所要求的结论 (a) 和 (b). 事实上, 注意到 $\delta \in R^N$, 立即有 (a) 成立. 而 (b) 则可由 (9.8) 式及 ζ_i 和 δ 的定义得出. 由于矩阵 $\big(D\mathcal{F}\big)(z)$ 的非奇异性, 故惟一性也是显然的.

下面估计计算复杂度：为了计算 $\mathcal{F}(z)$ 和 $\big(D\mathcal{F}\big)(z)$ 的非零项, $O(p^2N)$ 个 $R \pmod{p^{2m}}$ 上的算术运算是足够的. 而更进一步的 $2N$ 个行运算 (即 $O(N)^2$ 个算术运算) 给出 $\big(D\mathcal{F}\big)(z)^{-1} \cdot \mathcal{F}(z)$, 然后由

$${}^t\big(\zeta_0, \cdots, \zeta_{N-1}\big) = z - \big(D\mathcal{F}\big)(z)^{-1}\mathcal{F}(z)$$

知道还需要一个 $\big(R \pmod{p^{2m}}\big)^N$ 中的减法. 它当然等价于做 $R \pmod{p^{2m}}$ 中 N 个减法运算. 总之如果 p 是一个固定的小素数, $O(N)$ 个 $R \pmod{p^{2m}}$ 上的算术运算给出 $\zeta_i \pmod{p^{2m}}\,(\forall 0 \leqslant i < N)$, 证毕.

推论 9.1 设 E 为一椭圆曲线, 且 $j(E) \notin \mathbb{F}_{p^2}$, 记 Fr_p^iE 为 $E^{(i)}$, 而其典范提升记为 $E^{(i)\uparrow}$. 设 $\{a_n \in \mathbb{N}\}_{n=0}^{\infty}$ 是一个严格递增的序列, $a_0 = 1$, 对于 $0 \leqslant i < N$ 及 $n \geqslant 0$, 设 $z_{i,n} \in R$ 满足下列条件 (我们认为 $z_{N,n} = z_{0,n}$):

(i) $\pi(z_{i,0}) = Fr_p^ij(E)$;

(ii) $z_{i,n+1} \equiv z_{i,n} \pmod{p^{a_n}}$;

(iii) $\Phi_p(z_{i,n}, z_{i+1,n}) \equiv 0 \pmod{p^{a_n}}$.

则 $z_i := \lim_{n\to\infty} z_{i,n}$ 存在, 且对每个 $0 \leqslant i < N$, 有 $z_i = j\big(E^{(i)\uparrow}\big)$. 更进一步 $z_{i,n} \equiv j\big(E^{(i)\uparrow}\big) \pmod{p^{a_n}}$, 对所有的 $n \geqslant 0$.

证明 与上面命题 9.1 的证明类似, 可知方程组

$$
\begin{aligned}
&\Phi_p(Z_0, Z_1) = 0, \quad \cdots, \quad \Phi_p(Z_{N-2}, Z_{N-1}) = 0, \quad \Phi_p(Z_{N-1}, Z_0) = 0, \\
&\pi(Z_0) = j(E), \quad \cdots, \quad \pi(Z_{N-1}) = j(E^{(N-1)})
\end{aligned} \tag{9.9}
$$

在条件 $j(E) \notin \mathbb{F}_{p^2}$ 下至多有 1 个解. 因为 $E^{(i)\uparrow}$ 和 $E^{(i+1)\uparrow}$ 是 p-isogenous, 故

$$\left(j(E^{(0)\uparrow}), \cdots, j(E^{(N-1)\uparrow})\right)$$

是 (9.9) 式的一个解.

另一方面, 由 (ii) 知 $\{z_{i,n}\}_{n=1}^{\infty}$ 是一个柯西序列, 故 $z_i := \lim_{n\to\infty} z_{i,n}$ 存在. 于是由 (iii) 知 $\Phi_p(z_i, z_{i+1}) = 0$. 再由 (i) 和 (ii) 可知有 $\pi(z_i) = j\left(E^{(i)}\right)$, 从而 $(z_0, \cdots, z_{N-1})$ 是 (9.9) 式的一个解. 由惟一性知 $z_i = j\left(E^{(i)\uparrow}\right)$. 最后的断言易由非阿赋值的性质推出, 证毕.

注记 9.1 设 $M \in \mathbb{N}$, 假定需要 $j\left(E^{\uparrow}\right) \pmod{p^M}$, 我们可以进行如下:

Step 1: Put $v := \left[\log_2(M-1)\right] + 1$, $a_n := \left[2^{-(v-n)}M\right]$, 对 $0 \leqslant n \leqslant v$.

Step 2: Put $z_{i,0} := j\left(E^{(i)}\right) \in \mathbb{F}_q = R/pR$, 对 $0 \leqslant i \leqslant N-1$.

Step 3: 对 $n := 1, \cdots, v$, 利用 $z_{i,n-1}$ 和命题 9.1 计算 $z_{i,n} \in R/p^{a_n}R$ $(0 \leqslant i < N)$, 使得 $z_{i,n} \equiv z_{i,n-1} \pmod{p^{a_{n-1}}}$ 及 $\Phi_p(z_{i,n}, z_{i+1,n}) \equiv 0 \pmod{p^{a_n}}$. 则 $z_{0,v}$ 给出所期望的值.

引理 9.3 设 $\widetilde{E}$: $Y^2 = X^3 + \widetilde{A}X + \widetilde{B}$ 满足定理 9.1 中(i)至(iv)中条件之一, 则对于任何 $P \in \widetilde{E}[p] \cap \widetilde{E}(R^{ur}) - \{\mathcal{O}\}$, 有

$$\operatorname{ord}_p(\partial\psi_p)\left(\xi(P), \widetilde{A}, \widetilde{B}\right) = 1,$$

此处 $\partial = d/dX$.

证明 设 $Q \in \widetilde{E}[p] \cap \operatorname{Ker}\pi - \{\mathcal{O}\}$, 则由定理 9.1 中 (i) $\Longrightarrow$ (iv) 的证明过程知: P 和 Q 分别生成 p 阶循环群 $\widetilde{E}[p] \cap \widetilde{E}\left(R^{ur}\right)$ 和 $\widetilde{E}[p] \cap \operatorname{Ker}\pi$, 因此 p 次除子多项式分解为

$$
\begin{aligned}
\psi_p(X, \widetilde{A}, \widetilde{B}) = p \prod_{j=1}^{(p-1)/2} \left(X - \xi(jQ)\right) \times \prod_{i=1}^{(p-1)/2} \left(X - \xi(iP)\right) \\
\times \prod_{i=1}^{(p-1)/2} \prod_{j=1}^{p-1} \left(X - \xi(iP + jQ)\right)
\end{aligned}
$$

(在 K 的代数闭域中), 因此

$$\partial\psi_p(\xi(P),\widetilde{A},\widetilde{B}) = p\prod_{j=1}^{(p-1)/2}(\xi(P)-\xi(jQ))\times\prod_{i=2}^{(p-1)/2}(\xi(P)-\xi(iP))$$
$$\times\prod_{i=1}^{(p-1)/2}\prod_{j=1}^{p-1}(\xi(P)-\xi(iP+jQ)).$$

令 $\tau := -\xi/\eta$ 是在 $\mathcal{O}$ 处的局部参数, 并置 $t_j := \tau(jQ)$, 于是

$$\xi(jQ) = t_j^{-2} - \widetilde{A}t_j^2 + O(t_j^3),\quad \eta(jQ) = -t_j^{-3} + \widetilde{A}t_j + O(t_j^2),$$

故

$$\begin{aligned}\xi(iP+jQ) &= \left(\frac{-t_j^{-3}+\eta(iP)O(t_j)}{t_j^{-2}-\xi(iP)-O(t_j^2)}\right)^2 - \left(t_j^{-2}+O(t_j^2)\right) - \xi(iP)\\ &= \xi(iP) + 2\eta(iP)t_j + O(t_j^2).\end{aligned}$$

回顾 p 为奇素数且 $P \in \widetilde{E}[p]\cap\widetilde{E}(R^{ur})$, 从而 $\mathrm{ord}_p(\eta(iP)) = 0$, 对于 $1 \leqslant i \leqslant p-1$. 事实上, 因 $\widetilde{E}[p]\cap\widetilde{E}(R^{ur})$ 是由 P 生成的 p 阶循环群, 故 $\forall 1 \leqslant i \leqslant p-1$, $iP \in \widetilde{E}[p]\cap\widetilde{E}(R^{ur}) - \{\mathcal{O}\}$, 从而 $\mathrm{ord}_p(\eta(iP)) \geqslant 0$, 若 $\mathrm{ord}_p(\eta(iP)) > 0$, 则 mod p 约化有

$$\xi(iP)^2 + \widetilde{A}\xi(iP) + \widetilde{B} = 0 \pmod p.$$

可见 $\mathrm{ord}_p(\xi(iP)) = 0$ (否则 $\mathrm{ord}_p(\xi(iP)) > 0 \Longrightarrow \mathrm{ord}_p\widetilde{B} > 0 \Longrightarrow B \equiv \widetilde{B} \bmod p = 0$, 矛盾于 $AB \neq 0$), 从而 $(\xi(iP),\eta(iP)) = iP \pmod p$ 约化后属于 $E[2]$. 另一方面

$$p(\xi(iP),\eta(iP)) = \mathcal{O},$$

mod$p$ 约化后又得 (我们记 $\overline{(\alpha,\beta)} = \pi(\alpha,\beta)$)

$$p\overline{(\xi(iP),\eta(iP))} = \mathcal{O},$$

从而由 $2\overline{(\xi(iP),\eta(iP))} = \mathcal{O}$ 知 $\overline{(\xi(iP),\eta(iP))} = \mathcal{O}$, 故 $iP = (\xi(iP),\eta(iP)) \in \mathrm{Ker}\,\pi$. 这样有 $iP \in \widetilde{E}[p]\cap\mathrm{Ker}\,\pi - \{\mathcal{O}\} = G - \{\mathcal{O}\}$, 与 $H\cap G = \{\mathcal{O}\}$ 矛盾 (见定理 9.1 的证明过程).

另一方面, 可证明: 对于 $1 \leqslant i < j \leqslant (p-1)/2$, 有

$$\mathrm{ord}_p(\xi(iP) - \xi(jP)) = 0.$$

事实上, 由于 $iP, jP \in \widetilde{E}(R^{ur})\cap\widetilde{E}[p] - \{\mathcal{O}\}$, 故 $\xi(iP)$, $\eta(iP) \in R^{ur}$, 从而 $\mathrm{ord}_p(\xi(iP)$ $-\xi(jP)) \geqslant 0$. 若等号不成立, 则由

$$\eta(iP)^2 = \xi(iP)^3 + \widetilde{A}\xi(iP) + \widetilde{B},$$
$$\eta(jP)^2 = \xi(jP)^3 + \widetilde{A}\xi(jP) + \widetilde{B}$$

两式相减, 并 mod p 约化, 知 (因为 $\overline{\xi(iP)}=\overline{\xi(jP)}$)

$$\overline{\eta(iP)}=\pm\overline{\eta(jP)},$$

从而有

$$\overline{iP\pm jP}=\overline{iP}\pm\overline{jP}=\overline{(\xi(iP),\eta(iP))}\pm\overline{(\xi(jP),\eta(jP))}=(x,y)\pm(x,\pm y),$$

其中 $x=\overline{\xi(iP)}=\overline{\xi(jP)},y=\overline{\eta(iP)}$.

如果 $\overline{\eta(iP)}=\overline{\eta(jP)}$, 则上式表明

$$\overline{iP-jP}=(x,y)-(x,y)=0$$

$\Longrightarrow(i-j)P=iP-jP\in\operatorname{Ker}\pi\cap\widetilde{E}[p]$, 矛盾于 P 及 i,j 的选取.

若 $\overline{\eta(iP)}=-\overline{\eta(jP)}$, 则上式表明

$$\overline{iP+jP}=(x,y)+(x,-y)=0$$

$\Longrightarrow iP+jP=(i+j)P\in\operatorname{Ker}\pi\cap\widetilde{E}[p]$, 矛盾于 P 及 i,j 的选取.

最后, 注意到 $jQ\in\operatorname{Ker}\pi$, 从而 $\mathrm{ord}_pt_j\geqslant0$, 所以

$$\begin{aligned}\mathrm{ord}_p\big(\xi(P)-\xi(jQ)\big)&=-2\mathrm{ord}_pt_j,\\ \mathrm{ord}_p\big(\xi(P)-\xi(P+jQ)\big)&=\mathrm{ord}_p\big(-2\eta(P)t_j-O(t_j)^2\big)=\mathrm{ord}_pt_j,\\ \mathrm{ord}_p\big(\xi(P)-\xi(iP+jQ)\big)&=\mathrm{ord}_p\big(\xi(P)-\xi(iP)-2\eta(iP)tPj-O(t_j^2)\big)=0,\ \forall i\geqslant2,\end{aligned}$$

因为 $t_j=-t_{p-j},\forall1\leqslant j\leqslant p-1$, 故有

$$\mathrm{ord}_p\big((\partial\psi_p)(\xi(P),\widetilde{A},\widetilde{B})\big)=1+\sum_{j=1}^{(p-1)/2}(-2\mathrm{ord}_pt_j)+0+\sum_{j=1}^{p-1}\mathrm{ord}_pt_j=1.$$

证毕.

定理 9.2 设 $E/\mathbb{F}_q$ 是一条椭圆曲线, $j(E)\notin\mathbb{F}_{p^2}$, 其方程为

$$Y^2=X^3+AX+B.$$

设 $E^{(i)}$ 是其在 $\mathbb{F}_q$ 上的共轭, 其定义方程如下:

$$Y^2=X^3+\big(Fr_p^iA\big)X+Fr_p^iB.$$

令 $M\geqslant2$ 为一整数, 则存在一个算法产生下述: $\forall0\leqslant i<N$,

- 一条椭圆曲线 $E^{\langle\langle i\rangle\rangle}$: $Y^2=X^3+A^{\langle\langle i\rangle\rangle}X+B^{\langle\langle i\rangle\rangle}$;

• 一个多项式 $h^{\langle\langle i\rangle\rangle} \in R[X]$, 使得

$$h^{\langle\langle i\rangle\rangle}(X) \equiv \Bigg(\prod_{P\in(G^{\langle\langle i\rangle\rangle}-\{\mathcal{O}\}/\pm 1} (X-\xi(P))\Bigg), \quad (\text{mod } p^{M-1}),$$

其中 $G^{\langle\langle i\rangle\rangle} := E^{\langle\langle i\rangle\rangle}[p] \cap E^{\langle\langle i\rangle\rangle}(R^{ur})$.

它们满足以下条件:

(i) $j\big(E^{\langle\langle i\rangle\rangle}\big) \equiv j(E^{(i)\uparrow})$ $(\text{mod } p^M)$;

(ii) 群 $G^{\langle\langle i\rangle\rangle}$ 是一个阶为 p 的循环群, 其mod p 的约化是 $E^{(i)}[p]$;

(iii) $\pi\big(A^{\langle\langle i\rangle\rangle}\big) = A^{(i)}$ 且 $\pi\big(B^{\langle\langle i\rangle\rangle}\big) = B^{(i)}$.

整个算法要求 $O\big(N\log M\big)$ 个 R $(\text{mod } p^M)$ 上的运算及 $O(N^2)$ 个 $\mathbb{F}_q$ 上的运算 (此后, O 常数与 p 有关).

证明 首先, 计算 $A^{(i)} := Fr_q^i A$ 和 $B^{(i)} := Fr_q^i B$, 它们可由 $O(N)$ 个 $\mathbb{F}_q$ 上乘法获得. 取 $z_i \in R$, 使得 $\pi(z_i) = j\big(E^{(N-i)}\big)$, 重复应用命题 9.1 (共 $O\big(\log M\big)$ 次), 可以找到 $\zeta_i \in R$ 满足 $\Phi_p(\zeta_i, \zeta_{i+1}) \equiv 0$ $(\text{mod } p^M)$ 且 $\pi(\zeta_i) = j\big(E^{(N-i)}\big)$, 而由命题 9.1, 每一次需要 $O(N)$ 个 R $(\text{mod } p^M)$ 中运算, 故共要求 $O\big(N\log M\big)$ 个 R $(\text{mod } p^M)$ 中运算可求得这些 ζ_i.

取 $A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle} \in R$ 满足 $\pi\big(A^{\langle\langle i\rangle\rangle}\big) = A^{(i)}$, $\pi\big(B^{\langle\langle i\rangle\rangle}\big) = B^{(i)}$ 且 $j\big(E^{\langle\langle i\rangle\rangle}\big) = \zeta_{N-i}$. 这可由下述方法得出: 首先取定 $B^{\langle\langle i\rangle\rangle}$, 使得 $\pi\big(B^{\langle\langle i\rangle\rangle}\big) = B^{(i)}$, 然后取 $j\big(E^{\langle\langle i\rangle\rangle}\big) = \zeta_{N-i}$, 注意到 $j(A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}) = j(E^{\langle\langle i\rangle\rangle}) = 1728\frac{4A^3}{4A^3+27B^2}$, 故 $(\partial j/\partial A\big(A^{(i)}, B^{(i)}\big) \neq 0$ (因为 $AB \neq 0$, 因此 $A^{(i)}B^{(i)} \neq 0$), 于是利用 Hensel 引理知这样的 $A^{\langle\langle i\rangle\rangle}$ 存在, 且可由牛顿迭代, 在 $O\big(N\log M\big)$ 个 R $(\text{mod } p^M)$ 中运算内求得.

于是 (iii) 成立. 另外, $\Phi_p\big(j(E^{(N-i)\uparrow}), j(E^{(N-i+1)\uparrow})\big) = 0$ 且 $\pi\big(j(E^{(N-i)\uparrow})\big) = j\big(E^{(N-i)}\big)$. 由推论 9.1 的证明过程知 (i) 成立, 于是由定理 9.1 的 (iv)$\Longrightarrow$ (i) 知 (ii) 成立 (注意到 $G^{\langle\langle i\rangle\rangle} \cap \operatorname{Ker}\pi = \{\mathcal{O}\}$). 为了得到多项式 $h^{\langle\langle i\rangle\rangle}$, 我们研究 p 次除子多项式 ψ_p. 注意到: $\pi\big(\psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})\big) = cf(X)^p$, $f(X)$ 是首 1 的无平方因子多项式 $f \in \mathbb{F}_q[X]$ 且 $c \in \mathbb{F}_q^*$ (可参见文献 [20]), 事实上, 有

$$f(X) = \sum_{k=0}^{(p-1)/2} \frac{u_k}{u_{(p-1)/2}} X^k,$$

此处 u_k 是 $\psi_p\big(X, A^{(i-1)}, B^{(i-1)}\big)$ 中 X^{pk} 的系数, 无论如何, 均有

$$\operatorname{ord}_p\big(\partial\psi_p\big)\big(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}\big) \geqslant 1.$$

另一方面, $E^{\langle\langle i\rangle\rangle}$ 满足定理 9.1 的条件 (iv), 于是应用引理 9.3 知

$$\operatorname{ord}_p\big(\partial\psi_p\big)\big(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}\big) = 1,$$

从而 f 与 $\pi(1/p(\partial\psi_p)(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle}))$ 互素. 于是我们能够重复应用引理 9.1: 在其中取 $U(X) := \psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$, $t := 1$, 起始于 $u := 1$. 再由引理 9.2, 就得到 $\psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$ 的一个首 1 因子 $h(X)$. 注意到 $\psi_p(X, A^{\langle\langle i\rangle\rangle}, B^{\langle\langle i\rangle\rangle})$ 在 R^{ur} 中有 $(p-1)/2$ 个不同的根, 故得到 $h = h^{\langle\langle i\rangle\rangle}$, 因此 $O(\log M)$ 次应用引理 9.1足够获得 $h^{\langle\langle i\rangle\rangle} \pmod{p^{M-1}}$. 对于每个 i, 这个过程共要 $O(\log M)$ 个 $R \pmod{p^M}$ 上的算术运算 (由引理 9.1, O 常数与 p 有关, 因为应用 1 次引理 9.1, 则要 $O((\deg f + \deg U)^2)$ 次运算, 它是与 p 有关的), 于是共需要 $O(N \log M)$ 个 $R \pmod{p^M}$ 的运算即可算出全体的 $h^{\langle\langle i\rangle\rangle} \pmod{p^{M-1}}$, 对 $0 \leqslant i < N$, 定理得证.

§9.4 应用到点数的计算

在本节中, 我们给出计算点数的算法, 设 E 是 $\mathbb{F}_q$ 上的椭圆曲线, 下面的命题 9.3 告诉我们情形 $j(E) \in \mathbb{F}_{p^2}$ 是容易处理的, 因此假定 $j(E) \notin \mathbb{F}_{p^2}$. 在这个条件下, 可以应用定理 9.2 到 E. 我们计算 E 的典范提升的形式群上的 Verschiebung 的首项系数, 从而得出 Verschiebung 的迹.

首先开始于一条椭圆曲线的自同态诱导出的形式群上的自同态.

命题 9.2 *设 $\mathcal{E}/K$ 是一椭圆曲线且 $f \in \mathrm{End}_K(\mathcal{E})$ 的次数(degree)为 d. 记其在 $\mathcal{O}$ 处的局部参数为 τ, 假设 $f \bmod p$ 的约化 $\pi(f)$ 是可分的且 $f(\mathrm{Ker}\,\pi) \subset \mathrm{Ker}\,\pi$. 设 $\widehat{f}$ 是 f 在 $\mathcal{E}$ 的形式群 $\widehat{\mathcal{E}}$ 上诱导出的同态, 则*

$$\mathrm{Tr}(f) = c_1 + \frac{d}{c_1}, \tag{9.10}$$

其中 $\widehat{f}(\tau) = \sum_{n=1}^{\infty} c_n \tau^n$.

证明 因在 $\mathrm{End}(\mathcal{E})$ 中, f 满足

$$f \circ f - \mathrm{Tr}(f) f + d = 0,$$

故在 $\widehat{\mathcal{E}}$ 上,

$$(c_1^2 - \mathrm{Tr}(f) c_1 + d)\tau + O(\tau^2) = 0.$$

所有 τ 的系数必须为 0, 另一方面, $\pi(f)$ 的可分性表明 $\pi(c_1) \neq 0$, 所以 $c_1 \neq 0$, 这里用到了以下事实: 若 ϕ: $E_1 \to E_2$ 是定义在 K 上的一个非零 isogeny, 且 ϕ 是可分的, $\widehat{\phi}$: $\widehat{E}_1 \to \widehat{E}_2$ 是 ϕ 在形式群上诱导出的同态, 则 $\widehat{\phi}'(0) \neq 0$. 证明如下: 设 ω 是 E_2/K 上的不变微分, 而 $\omega(T)$ 是对应的形式群 $\widehat{E}_2$ 上不变微分. 因为 ϕ 是可分的, 故由命题 3.6 知 $\phi^*\omega \neq 0$. 于是应用推论 7.1 有

$$0 \neq \omega \circ \widehat{\phi}(T) = \widehat{\phi}'(0)\omega(T),$$

从而 $\widehat{\phi}'(0) \neq 0$. 将上面事实应用到 $\phi = \pi(f)$, 则可知 $\widehat{\phi} = \widehat{\pi(f)} = \pi(\widehat{f})$ 满足 $\widehat{\phi}'(0) = \pi(\widehat{f})'(0) \neq 0$, 即 $\pi(c_1) \neq 0$.

从而 $\mathrm{Tr}\ (f) = c_1 + \frac{d}{c_1}$, 证毕.

注 9.1 命题 9.2 中条件 $f(\mathrm{Ker}\,\pi) \subset \mathrm{Ker}\,\pi$ 是为了保证 $\pi(f)$ 是 $E \pmod p$ 上的同态, 见下面的交换图表:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E_1(K) & \longrightarrow & E(K) & \xrightarrow{\pi} & \widetilde{E}(k) & \longrightarrow & 0 \\ & & \downarrow f & & \downarrow f & & \downarrow \pi(f) & & \\ 0 & \longrightarrow & E_1(K) & \longrightarrow & E(K) & \xrightarrow{\pi} & \widetilde{E}(k) & \longrightarrow & 0 \end{array}$$

为了 $\pi(f)$ 有合理定义: 即当 $P, P_1 \in E(K)$, 且 $\widetilde{P} = \widetilde{P_1}$ 时, 有 $\pi(f)(\widetilde{P}) = \pi(f)(\widetilde{P_1})$, 我们要求 $f(\mathrm{Ker}\,\pi) \subset \mathrm{Ker}\,\pi$, 事实上, 若如此, 则

$$\pi(f)(\widetilde{P}) = \pi\big(f(P)\big), \qquad \pi(f)(\widetilde{P_1}) = \pi\big(f(P_1)\big).$$

因 $\widetilde{P} = \widetilde{P_1}$, 所以 $P - P_1 \in \mathrm{Ker}\,\pi$, 所以 $f(P - P_1) \in \mathrm{Ker}\,\pi \Longrightarrow \pi\big(f(P - P_1)\big) = 0$, 即 $\pi\big(f(P)\big) = \pi\big(f(P_1)\big)$, $\pi(f)(\widetilde{P}) = \pi(f)(\widetilde{P_1})$, 亦即 $\pi(f)$ 定义合理, 从而它是 $\widetilde{E}(k)$ 到 $\widetilde{E}(k)$ 的同态.

命题 9.3 *设 $q = p^N$, $E:\ Y^2 = X^3 + AX + B$ 是在 $\mathbb{F}_q$ 上的椭圆曲线, 又 $j(E) \in \mathbb{F}_{p^2}$, 则 $\#E(\mathbb{F}_q)$ 能够用 $\mathbb{F}_q$ 上 $O(N)$ 个算术运算和 $O(N^{1+\mu})$ 个比特运算决定出来.*

证明 定义 $m \in \mathbb{Z}$, 使得 $p^m = \#\mathbb{F}_p\big(j(E)\big)$, 由假设 $j(E) \in \mathbb{F}_{p^2}$ 知 $m = 1$ 或 2. 于是存在一条椭圆曲线 $E':\ Y^2 = X^3 + A'X + B'$, 它定义在 $\mathbb{F}_{p^m}$ 上且在 $\mathbb{F}_q$ 上同构于 E. 我们能够获得这样的 E' 如下: 注意我们能够用 $\mathbb{F}_q$ 上的 $O(N)$ 个算术运算决定 E 是否在 $\mathbb{F}_q$ 上同构于 E'. 例如, 在 $AB \neq 0$ 时, 检验是否有 $j(E) = j(E')$ 且 $(\frac{A/B}{A'/B'})^{(q-1)/2} = 1$. 其余情形类似处理. 设 $E_0/\mathbb{F}_{p^m}$ 是任意满足 $j(E_0) = j(E)$ 的椭圆曲线, 它能够用 $\mathbb{F}_{p^m}$ 上 $O(1)$ 个运算构造出来 (见文献 [12] III 1.4(c)). 我们可以取 E_0 作为 E', 如果 E_0 在 $\mathbb{F}_q$ 上同构于 E. 否则, 取 E_0 在 $\mathbb{F}_{p^m}$ 上的 twist 作为 E', 它也能够在 $O(1)$ 个运算中构造出来. 于是显然有

$$\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q),$$

从而, 如果能得到 $\mathrm{T}_{N/m}$(此处 $\mathrm{T}_i := \mathrm{Tr}\, Fr^i_{p^m}\big|_{E'}$), 则

$$\#E(\mathbb{F}_q) = \#E'(\mathbb{F}_q) = q + 1 - \mathrm{T}_{N/m} \quad (\text{注意} m|N).$$

值 $T_1 = 1 + p^m - \#E'(\mathbb{F}_{p^m})$ 可以借助于例如穷举法 (因 p 不大) 在 $O(1)$ 个 $\mathbb{F}_{p^m}$ 上的运算得出, 从而由关系式

$$T_{i+2} - T_1 T_{i+1} + p^m T_i = 0, \quad T_0 = 2$$

可以得出 $T_{N/m}$. 由于 $|T_i| \leqslant 2p^{im/2}$, 可见从 T_1 得出 $T_{N/m}$ 只要 $O\big(N^{1+\mu}\big)$ 个 bit 运算即可, 证毕.

注 9.2 我们用到下述事实: 设 $E: Y^2 = X^3 + AX + B$, $E': Y'^2 = X'^2 + A'X' + B'$ 是 2 条椭圆曲线 (定义在 $\mathbb{F}_q$ 中), 如果 $j(E) = j(E')$ 且 $(\frac{A/B}{A'/B'})^{(q-1)/2} = 1$, 则 E 与 E' 在 $\mathbb{F}_q$ 上是同构的: 因为 $j(E) = j(E')$, 故 E 与 E' 在 $\overline{\mathbb{F}_q}$ 上同构. 同构映射有以下形式:

$$x = u^2x', \quad y = u^3y', \quad 对某个\ u \in \overline{\mathbb{F}_q}^*.$$

该同构定义在 $\mathbb{F}_q$ 上当且仅当 $u \in \mathbb{F}_q^*$, 但由此易知

$$u^4A' = A, \qquad u^6B' = B,$$

从而

$$u^2 = \frac{A/B}{A'/B'}, \quad u \in \mathbb{F}_q^* \iff u^{q-1} = 1 \iff \left(\frac{A/B}{A'/B'}\right)^{(q-1)/2} = 1.$$

以下假定 $j(E) \notin \mathbb{F}_{p^2}$, 利用与定理 9.2 相同的记号, 更进一步, 设 $E^{(i)\uparrow}$ 是 $E^{(i)}$ 的典范提升. 不失一般性, 可设 $E^{(i)\uparrow}: Y^2 = X^3 + A^{(i)\uparrow}X + B^{\langle\langle i\rangle\rangle}$, $A^{(i)\uparrow} \in R$. 为了记号方便, 置 $B^{(i)\uparrow} := B^{\langle\langle i\rangle\rangle}$. 令

$$G^{(i)} := E^{(i)\uparrow}[p] \bigcap E^{(i)\uparrow}(R^{ur})$$

是一个 p 阶循环群. 令 $V_p^{(i)}$ 是 $Fr_p \in \mathrm{Isog}(E^{(i-1)}, E^{(i)})$ 的对偶同种,$V_p^{(i)}$ 可提升到 $V_p^{(i)\uparrow} \in \mathrm{Isog}(E^{(i)\uparrow}, E^{(i-1)\uparrow})$, 我们研究它在形式群上的作用.

命题 9.4 *设 $\tau_i(X,Y) := -X/Y$ 是 $E^{(i)\uparrow}$ 在 $\mathcal{O}$ 处的局部参数, 假设 $A^{(i)\uparrow}$, $B^{(i)\uparrow}$ 及*

$$h^{(i)\uparrow}(X) := \prod_{g \in (G^{(i)} - \{\mathcal{O}\})/\pm 1} (X - \xi(g))$$

被给定, 定义 $c_1^{(i)} \in R$ 如下:

$$\tau_{i-1} \circ V_p^{(i)\uparrow} = c_1^{(i)}\tau_i + O(\tau_i^2),$$

则能够在 $O(1)$ 个 R 上的算术运算内得出 ${c_1^{(i)}}^2$ 的值.

证明 因为 $V_p^{(i)\uparrow}$ 是 $V_p^{(i)}$ 的一个提升, 图 9.2 中的长方形是交换的:

设 $v \in \mathrm{Isog}\big(E^{(i)\uparrow}, E^{(i)\uparrow}/G^{(i)}\big)$ 是由 Vélu 构造的同种, 即

$$v(X,Y) := \Big(X + \sum_{g \in G^{(i)} - \{\mathcal{O}\}} \Big(\xi\big((X,Y)+g\big) - \xi(g)\Big), \sum_{g \in G^{(i)}} \eta\big((X,Y)+g\big)\Big),$$

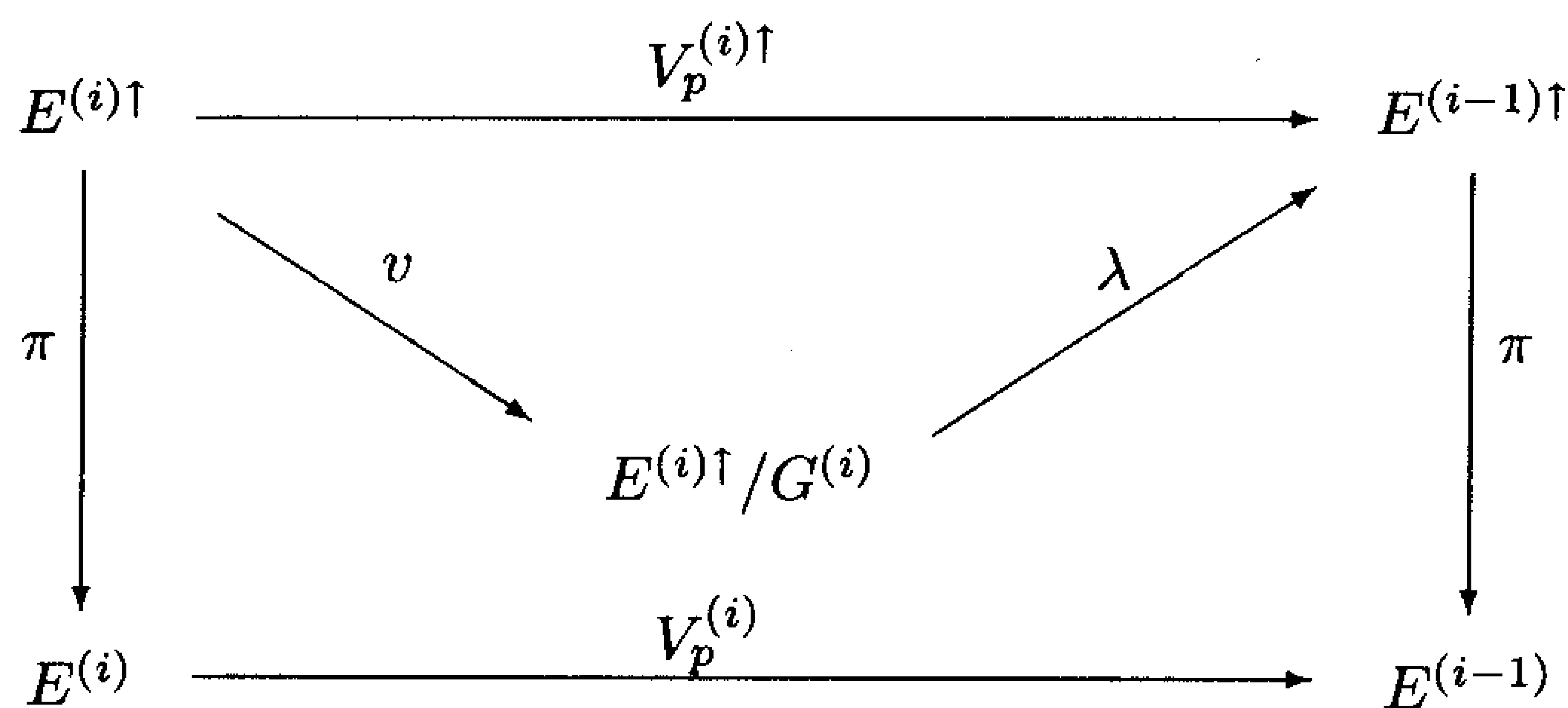


图 9.2

其中 $(X,Y)+g$ 是椭圆曲线上点的相加. Vélu 的公式也给出了 $E^{(i)\uparrow}/G^{(i)}$ 的 Weierstrass 方程：令 s_i 是 $h^{(i)\uparrow}$ 中 $X^{(p-1)/2-i}$ 的系数, 则 $E^{(i)\uparrow}/G^{(i)}$ 是

$$Y^2 = X^3 + \alpha_i X + \beta_i,$$

其中

$$\begin{aligned}\alpha_i &:= A^{(i)\uparrow} - 5 \sum_{g\in G^{(i)}-\{\mathcal{O}\}} \left(3\xi(g)^2 + A^{(i)\uparrow}\right) = (6-5p)A^{(i)\uparrow} - 30(s_1^2 - 2s_2),\\ \beta_i &:= B^{(i)\uparrow} - 7 \sum_{g\in G^{(i)}-\{\mathcal{O}\}} \left(5\xi(g)^3 + 3A^{(i)\uparrow}\xi(g) + 2B^{(i)\uparrow}\right)\\ &= (14-14p)B^{(i)\uparrow} - 70(-s_1^3 + 3s_1s_2 - 3s_3) + 42A^{(i)\uparrow}s_1,\end{aligned}$$

其中, 若 $p=5$, 则认为 $s_3=0$.

因为 $V_p^{(i)\uparrow}$ 可分, 且 $\operatorname{Ker} v = \operatorname{Ker} V_p^{(i)\uparrow} = G^{(i)}$, 于是存在 $\lambda \in \operatorname{Isog}\left(E^{(i)\uparrow}/G^{(i)}, E^{(i-1)\uparrow}\right)$, 使得图 9.2 中的三角形是可交换的 (见定理 3.10). 但 $\deg(V_p^{(i)\uparrow}) = \deg(v)\deg(\lambda)$ 表明 λ 是一个同构 (因 $\deg(V_p^{(i)\uparrow}) = \deg(v) = p$, 故 $\deg(\lambda)=1$), 所以 λ 由下式给定：

$$\lambda(X,Y) = (\gamma_i^2 X, \gamma_i^3 Y), \quad \text{对某个}\gamma_i \in R.$$

映射 v 诱导出一个形式群之间的同态 $\widehat{v}$, 由 Vélu 的结果知 $\widehat{v}$ 的首项系数是 1, 而 $\widehat{\lambda}(t) = t/\gamma_i$, 从而 $\widehat{V}_p^{(i)\uparrow}$ 的首项系数是 $1/\gamma_i$, 再比较

$$\tau_{i-1} \circ V_p^{(i)\uparrow} = c_1^{(i)}\tau_i + O(\tau_i^2)$$

知 $c_1^{(i)} = 1/\gamma_i$. 又 λ：$E^{(i)\uparrow} \to E^{(i-1)\uparrow}$ 给出

$$B^{(i-1)\uparrow} = \beta_i\gamma_i^6, \qquad A^{(i-1)\uparrow} = \alpha_i\gamma_i^4,$$

所以

$$\left(c_1^{(i)}\right)^2 = \gamma_i^{-2} = \frac{\beta_i/\alpha_i}{B^{(i-1)\uparrow}/A^{(i-1)\uparrow}}.$$

证毕.

定理 9.3 设 $q := p^N$, $E/\mathbb{F}_q$ 是一椭圆曲线且 $j(E) \notin \mathbb{F}_{p^2}$. 存在一个算法可以确定 $\#E(\mathbb{F}_q)$, 其时间复杂度是 $O\big(N\log N\big)$ 个 $R \pmod{p^N}$ 上的运算加上 $O(N)$ 个 $\mathbb{F}_q$ 上的运算.

证明 设 $c_1^{(i)}$ 如命题 9.4, 则

$$\mathrm{Tr}(\mathbb{F}_q) = \mathrm{Tr}\big(V_p^{(0)\uparrow} \circ V_p^{(N-1)\uparrow} \circ \cdots \circ V_p^{(2)\uparrow} \circ V_p^{(1)\uparrow}\big).$$

于是由命题 9.2 和 9.4 知

$$\mathrm{Tr}(\mathbb{F}_q) = c + \frac{q}{c},$$

其中 $c := \prod_{i=0}^{N-1} c_1^{(i)}$, 但是 $|\mathrm{Tr}Fr_q| \leqslant 2\sqrt{q}$, 因此, $c \bmod p^{N/2+\alpha}$(例如, $\alpha := 3$) 就足以获得 $\mathrm{Tr}Fr_q$, 从而代替 $A^{(i)\uparrow}$ 和 $h^{(i)\uparrow}$, 我们可以用定理 9.2 给出的 $A^{\langle\langle i\rangle\rangle}$ 和 $h^{\langle\langle i\rangle\rangle}$, 其中 $M := N/2 + \alpha + 1$. $A^{\langle\langle i\rangle\rangle}$ 和 $h^{\langle\langle i\rangle\rangle}$ 的计算需要 $O\big(N\log M\big)$ 个运算. 由命题 9.4, 可在 $O(N)$ 个运算中得出 c^2. 另一方面, 设 C_1 是 $(X^3+AX+B)^{(p-1)/2} \in \mathbb{F}_q[X]$ 中 X^{p-1} 的系数, 定义 $C_n\,(n \geqslant 2)$ 如下:

$$C_n := C_{n-1}C_1^{p^{n-1}},$$

则与文献 [12] 定理 V.4.1 的证明同样可证得

$$C_N \equiv c \pmod{p}.$$

很显然 C_N 能够用 $O(N)$ 个 $\mathbb{F}_q$ 中运算计算出来, 因此可以利用 Hensel 引理和牛顿迭代从 C_N 和 $c^2 \pmod{p^M}$ 中得到 $c \pmod{p^M}$, 这需要 $O\big(\log N\big)$ 个 R/p^MR 上的运算.

现令 v 是惟一的整数, 满足 $|v| \leqslant 2\sqrt{q}$ 且 $v \equiv c \pmod{p^M}$, 则 $\#E(\mathbb{F}_q) = q+1-v$, 证毕.

注记 9.2 $R \pmod{p^N}$ 上一个算术运算需要 $O\big(N^{2\mu}\big)$ 个比特运算, 而一个 $\mathbb{F}_q$ 上的算术运算需要 $O\big(N^{\mu}\big)$ 个比特运算, 所以由推论 9.1, 我们看到整个算法可在 $O\big(N^{2\mu+1}\big)$ 个比特运算中完成.

第十章 Satoh 的算法及其实现

在前面, 我们已经讨论了 p-adic 域上椭圆曲线的基本理论和有限域上椭圆曲线的基本性质, 然后给出了 Satoh 算法的理论基础. 现在, 我们讨论其具体实现.

§10.1 局部域及其上一些算法的实现

我们已经讨论了有关 p-adic 数域的基本理论, 现在我们回顾一下.

设 π_n 是从 $\mathbb{Z}/p^{n+1}\mathbb{Z}$ 到 $\mathbb{Z}/p^n\mathbb{Z}$ 的投射, 它是一个环同态, 则我们可以从另一个角度给出 p-adic 整数一个形式的定义:

定义 10.1 一个 p-adic整数是一个序列 $x=(x_1,x_2,\cdots,x_n,\cdots)$, 使得 $x_n\in\mathbb{Z}/p^n\mathbb{Z}$ 且 $\pi_n(x_{n+1})=x_n, \forall\, n\geqslant 1$. p-adic整数的环记为 $\mathbb{Z}_p$.

$\mathbb{Z}_p$ 中的和与积以自然的对应坐标方式相加、相乘得出. $\mathbb{Z}_p$ 是非分歧的离散赋值环, 其惟一非零素理想是 $p\mathbb{Z}_p$, 剩余类域 $\mathbb{Z}_p/p\mathbb{Z}_p$ 是 $\mathbb{F}_p$.

我们扩充 π_n 的定义: 从 $\mathbb{Z}_p$ 到 $\mathbb{Z}/p^n\mathbb{Z}$: $x\mapsto x_n$. 显然, 一旦 x_n 知道了, 则易知 x_k, $\forall\, k<n$, 这只要将 x_n 投影到 $\mathbb{Z}/p^k\mathbb{Z}$ 即可. 令 $\pi=\pi_1$, 于是 π 也可考虑作到 $\mathbb{F}_p$ 的投影. $\mathbb{Z}_p$ 的可逆元是那些不在 $p\mathbb{Z}_p$ 中者, 即那些使得 $\pi(x)\neq 0$ 的 x.

现设 $q=p^d$, p 为素数, 而 $f(t)$ 是 $\mathbb{Z}_p[t]$ 中一个次数为 d 的首 1 多项式, 且使得多项式 $\pi(f)\in\mathbb{F}_p[t]$ 是不可约的.

定义 10.2 环 $\mathbb{Z}_q$ 是 $\mathbb{Z}_p[t]$ 模去 $f(t)$ 生成的理想所得, 即

$$\mathbb{Z}_q:=\mathbb{Z}_p[t]/\big(f(t)\big).$$

于是 $\mathbb{Z}_q$ 的一个元素 a 可以表示为一个多项式 $a_{d-1}t^{d-1}+\cdots+a_1t+a_0$, 其中, $\forall i, a_i\in\mathbb{Z}_p$, $\mathbb{Z}_q$ 中的和与积是通常多项式的和与积再模去 $f(t)$.

注意 $\mathbb{Z}_q$ 包含 $\mathbb{Z}_p$ 作为一个子环: 置 $a_1=a_2=\cdots=a_{d-1}=0$. 更进一步, $\mathbb{Z}_q$ 是一个非分歧的离散赋值环, 仅有的非零素理想是 $p\mathbb{Z}_q$, 而剩余类域 $\mathbb{Z}_q/p\mathbb{Z}_q$ 是 $\mathbb{F}_q$, 事实上, 这些条件就刻画了 $\mathbb{Z}_q$.

我们可以以自然方式扩充 π_n 的定义到 $\mathbb{Z}_q$, 而 π 可以考虑为到 $\mathbb{F}_q$ 的投影. 以后, 我们应用记号 mod p^n 表示对一个给定的关系模去 $p^n\mathbb{Z}_q$. $\mathbb{Z}_q$ 中的可逆元是那些使得 $\pi(x)\neq 0$ 的 x.

定义 10.3 在 $\mathbb{F}_q$ 上的 “小Frobenius” 是域的自同构 σ : $x\mapsto x^p$, 它固定子域 $\mathbb{F}_p$.

为了定义“小提升 Frobenius” $\Sigma:\ \mathbb{Z}_q \to \mathbb{Z}_q$, 需要给出某些定义, 需要指出的是, 尽管 Σ 能够按照下面给出的方法计算, 但速度很慢. Satoh 算法的一个巧妙之处就是避免计算 Σ.

定义 10.4 Teichmüller提升 $\omega:\mathbb{F}_q \to \mathbb{Z}_q$ 定义如下: $\omega(0)=0$, 对于非零的 x, $\omega(x)$ 是 $\mathbb{Z}_q$ 中惟一的 $(q-1)$ 次单位根, 使得 $\pi(\omega(x))=x$.

注意 Teichmüller 提升能够利用 Hensel 引理和牛顿迭代 (对函数 $f(x)=x^{q-1}-1$) 得出. 下面给出 $\mathbb{Z}_q$ 中元素的一个分解.

定义 10.5 $x\in\mathbb{Z}_q$ 的半 Witt 分解是指惟一的序列 $(x_i)_{i\geqslant 0}$, $x_i\in\mathbb{F}_q$, 使得 $x=\sum_{i\geqslant 0}\omega(x_i)p^i$.

坐标 x_i 显然可以一个接一个地计算出来: $x_0=\pi(x)$, $x_1=\pi(\frac{x-\omega(x_0)}{p}),\cdots$, 等等. 现在我们可以定义“小提升 Frobenius” Σ, 它是 σ 到 $\mathbb{Z}_q$ 的提升, 即 $\pi(\Sigma)=\sigma$.

定义 10.6 $\Sigma:\ \mathbb{Z}_q\to\mathbb{Z}_q$ 定义如下: 对任意 $x\in\mathbb{Z}_q$, 令 $(x_i)_{i\geqslant 0}$ 是其半 Witt 分解, 则 $\Sigma(x)$ 是 $\mathbb{Z}_q$ 的元素, 其半 Witt 分解为 $(x_i^p)_{i\geqslant 0}$, 换言之,

$$\Sigma(x)=\sum_{i\geqslant 0}\omega(x_i^p)p^i=\sum_{i\geqslant 0}\omega(x_i)^p p^i.$$

注意: Σ 并不像 σ 一样为一个 p 次幂映射.

在 p-adic 整数中进行计算, 只可能进行到一定的精度, 以后, 我们称计算 $a\in\mathbb{Z}_p$ 到精度 n, 是指由一个近似值 $a_n\in\mathbb{Z}/p^n\mathbb{Z}$ 代表 a, 而环运算是 modulo p^n.

一个可逆元 $a\in\mathbb{Z}_p$ 的逆可以通过一个简单的牛顿迭代: $x\longleftarrow x-x(ax-1)$ 而得到, 初始化在 $1/\pi(a)\in\mathbb{F}_p$ 处. 类似地, 表示 $a=a_{d-1}t^{d-1}+\cdots+a_0\in\mathbb{Z}_q$ 到某个精度 n, 可以储存序列 $(\pi_n(a_{d-1}),\cdots,\pi_n(a_0))$. 空间要求是 $s=O(nd\log p)$, 2 个元素加减的时间是 $O(s)$. 多项式 $f(t)$ 的选取应是使它为稀疏的, 且系数很小, 从而 mod $f(t)$ 只要少量运算即可. 由于 p-adic 域中的许多运算都离不开牛顿迭代, 所以下面专门讨论一下它:

设 R 是任意 p-adic 环, 则牛顿迭代可以从一个多项式的近似根得出一个近似程度更高的根. 记: $p^k|x$, 若 $x\equiv 0 \mod p^k$, 于是 $p^{-k}x\in R$; 又记 $p^k\|x$, 若 $p^k|x$ 但 $p^{k+1}\nmid x$, 于是 $p^{-k}x\in R$ 是可逆元.

设 $x\in R$, $f\in R[t]$, $n>k$, 使得 $p^k\|f'(x)$, $p^{n+k}|f(x)$. 在这些假设条件下, 说 x 是 f 的一个近似根, 其精度为 n, 如果存在 f 的精确根 $y\in R$, 使 $x\equiv y \pmod{p^n}$.

首先给出下述引理, 它表明如何通过牛顿迭代从一个精度 n 的根得出一个精度 $2n-k$ 的根.

引理 10.1 设 $x\in R$, $f\in R[t]$, $n>k$, 使得 $p^k\|f'(x)$, $p^{n+k}|f(x)$, 置

$$\Delta=\frac{p^{-k}f(x)}{p^{-k}f'(x)},\quad y=x-\Delta,$$

则 $y \equiv x \pmod{p^n}$, $p^{2n}|f(y)$, $p^k\|f'(y)$.

证明 显然 $p^n|\Delta$, 故 $y \equiv x \pmod{p^n}$, 由 Taylor 展开知

$$f(y) = f(x) - \Delta f'(x) + \Delta^2\psi(x),$$

$\psi(x)$ 是一个系数在 R 中的多项式. 因 $p^{2n}|\Delta^2$, 有

$$f(y) \equiv f(x) - \Delta f'(x) \equiv 0 \pmod{p^{2n}}.$$

最后, 因 $y \equiv x \pmod{p^n}$, 可知 $f'(y) \equiv f'(x) \pmod{p^n}$, 因 $p^k\|f'(x)$ 且 $n > k$, 故 $p^k\|f'(y)$, 证毕.

重复引用上述引理, 就可以给出一个算法, 它可以计算一个多项式的根到任意精度 (只要初始近似根足够好).

(算法 10.1) Procedure Newton Iterations

Inputs:

- 一个多项式 $f \in R[t]$;
- 一个起始解 $x_0 \in R$ 及整数 k, $p^k\|f'(x_0), p^{2k+1}|f(x_0)$;
- 一个期望的精度 n.

Output: 一个近似根 $x \in R$, $x \equiv x_0 \pmod{p^{k+1}}$ 且 $p^{n+k}|f(x)$.

1. If $n \leqslant k+1$ then $y \leftarrow x_0$; goto 5;
2. $n' \leftarrow [\frac{n+k}{2}]$;
3. $x \leftarrow$Newton Iterations (f, x_0, k, n');
4. $y \leftarrow x - \frac{p^{-k}f(x)}{p^{-k}f'(x)}$;
5. Return y.

为了使算法有效, 在算法的每一步都以最小可能精度工作是十分重要的. 特别地, 应当尽可能在每一次递归运用牛顿迭代时降低精度要求: 为了达到所期望的精度 n 所需递归次数是 $\log n$, 故如果所有运算都在精度 n 的水平上进行, 则总耗时将是 $O\big(M(n)\log n\big)$, 此处 $M(n)$ 是乘法的时间, 而如果用全精度做最上面的迭代, 用约一半的精度做第一次递归, 用约 $\frac{1}{4}$ 精度作第 2 次递归等等, 则耗时为 $O\big(M(n)\big)$.

更进一步, 在计算改进的根 $y = x - f/f'$ 时, 我们可以减少某些计算的精度要求约一半. 最低要求精度如下所示: 我们将写 $x + O(p^n)$ 来记任意 $y \equiv x \pmod{p^n}$, 例如 $xy + O(p^n)$ 可以理解为计算到精度 n 的乘积 xy.

当一个元素 $a \in R$ 已知有精度 n 时, 则乘积 $p^k a$ 具有精度 $n+k$(在下述意义下: $p^k\big(a + O(p^n)\big) = p^k a + O(p^{n+k})$). 反之, 当 a 已知具有精度 n 且 $p^k|a$ 时, $k \leqslant n$,

则 $p^{-k}a$ 具有精度 $n-k$. 在实际中, 用 p^k 乘除可快速计算, 即右 (左) 移位 (当 $p=2$ 时).

现在牛顿迭代可计算 $y = x - \Delta + O(p^{2n-k})$, 此处

$$\Delta = \left(\frac{\big(f(x)+O(p^{2n})\big)\cdot p^{-n-k}+O(p^{n-k})}{\big(f'(x)+O(p^n)\big)\cdot p^{-k}+O(p^{n-k})}+O(p^{n-k})\right)\cdot p^n + O(p^{2n-k}).$$

§10.2 Frobenius 同态及典范提升

设 $E/\mathbb{F}_q$ 是一条椭圆曲线, $q=p^d$, 众所周知, 可以通过计算该椭圆曲线的 q 次 Frobenius 同态的迹 c 得到 $E(\mathbb{F}_q)$ 的阶, 即

$$\#E(\mathbb{F}_q) = q+1-c, \qquad |c| \leqslant 2\sqrt{q}.$$

而在 $\mathbb{F}_q$ 上的 "小 Frobenius" σ 也可能扩充到 E 上的点 (x,y):

$$\begin{array}{cccc} \sigma: & E & \longrightarrow & E^{\sigma} \\ & (x,y) & \longmapsto & \big(\sigma(x),\sigma(y)\big), \end{array}$$

其中 E^{σ} 是将 σ 应用到 E 的系数而得到的方程所定义的椭圆曲线, 则 σ 是一个次数为 p 的纯不可分的同种, 而称之为 "小 Frobenius". 重复 d 次后, 又回到起始曲线 E, 从而给出了一个同种的闭链. 写 $E_0 = E, E_{d-1} = E^{\sigma}, E_{d-2} = E^{\sigma^2}, \cdots, \sigma_{d-1}, \sigma_{d-2}, \cdots$ 是对应的同种, 则有

$$E_0 \xrightarrow{\sigma_{d-1}} E_{d-1} \xrightarrow{\sigma_{d-2}} E_{d-2} \longrightarrow \cdots \xrightarrow{\sigma_1} E_1 \xrightarrow{\sigma_0} E_0.$$

定义 10.7 *在 E 上的 q 次Frobenius是椭圆曲线 E 的自同态 $F=\sigma_0\circ\cdots\circ\sigma_{d-1}$.*

注意: F 在 $\mathbb{F}_q$ 上的作用是平凡的, 但在其扩域上的作用是非平凡的. 相同地, 若有 $\mathcal{E}/\mathbb{Z}_q$, 则 $\mathbb{Z}_q$ 上的 "小 Frobenius" Σ 可以扩充到一个从 $\mathcal{E}$ 到 $\mathcal{E}^{\Sigma}$ 的映射, 重复这个运算 d 次, 又回到起始曲线, 从而有一个曲线和同种的闭链.

下面回顾一下模方程的一些基本事实: 模方程 $\Phi_p(X,Y)$ 是在每个变元上次数为 $p+1$ 的对称多项式, 具有整系数, 且有以下性质: 2 条椭圆曲线 $E/\mathbb{F}_q$ 和 $E'/\mathbb{F}_q$ 间能够存在一个次数 l 的循环同种当且仅当 $\Phi_l\big(j(E),j(E')\big)=0$.

模方程满足 Kronecker 同余关系式

$$\Phi_p(X,Y) \equiv (X^p-Y)(X-Y^p) \pmod{p}.$$

模多项式的系数随 p 的增长而极快地增长.

$$\begin{aligned}\Phi_2(X,Y) = {} & X^3+Y^3-X^2Y^2+c_1(XY^2+X^2Y) \\ & -c_2(X^2+Y^2)+c_3XY+c_4(X+Y)-c_5,\end{aligned}$$

其中

$$c_1 = 1488,\ c_2 = 162000,\ c_3 = 40773375,\ c_4 = 8748000000,\ c_5 = 157464000000000.$$

$$\begin{aligned}\Phi_3(X,Y) = {} & X^4 + Y^4 - X^3Y^3 + d_1(X^3Y^2 + X^2Y^3) - d_2(X^3Y + XY^3) \\ & + d_3(X^3 + Y^3) + d_4X^2Y^2 + d_5(X^2Y + XY^2) + d_6(X^2 + Y^2) \\ & - d_7XY + d_8(X + Y),\end{aligned}$$

其中

$$d_1 = 2232,\ d_2 = 1069956,\ d_3 = 36864000,\ d_4 = 2587918086,\ d_5 = 8900222976000,$$

$d_6 = 452984832000000, d_7 = 770845966336000000, d_8 = 1855425871872000000000.$

下面的定理属于 Deuring, Lubin, Serre 和 Tate, 它告诉我们可以将 $\mathbb{F}_q$ 上的一椭圆曲线 E 典范提升到 $\mathbb{Z}_q$ 上的一椭圆曲线 $\mathcal{E}$, 且 $\mathcal{E}$ 是与 E 有相同的自同态环的惟一提升.

定理 10.1　*设 $E/\mathbb{F}_q$ 为椭圆曲线, $j = j(E) \in \mathbb{F}_q \setminus \mathbb{F}_{p^2}$, 则存在惟一的 $J \in \mathbb{Z}_q$, 使得*

$$\Phi_p\big(J, \Sigma(J)\big) = 0,\ J \equiv j \pmod p,$$

并且 J 是 E 的典范提升 $\mathcal{E}$ 的 j 不变量.

于是有

$$\begin{array}{ccccccccccc}
\mathcal{E}_0 & \xrightarrow{\Sigma_{d-1}} & \mathcal{E}_{d-1} & \xrightarrow{\Sigma_{d-2}} & \mathcal{E}_{d-2} & \longrightarrow & \cdots & \xrightarrow{\Sigma_1} & \mathcal{E}_1 & \xrightarrow{\Sigma_0} & \mathcal{E}_0 \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & & & \downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\
E_0 & \xrightarrow{\sigma_{d-1}} & E_{d-1} & \xrightarrow{\sigma_{d-2}} & E_{d-2} & \longrightarrow & \cdots & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_0} & E_0
\end{array}$$

及

$$\begin{array}{ccc}
\mathcal{E} & \xrightarrow{\mathcal{F}} & \mathcal{E} \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} \\
E & \xrightarrow{F} & E
\end{array}$$

考虑上述图表的对偶同种, 有

$$\begin{array}{ccccccccc}
\mathcal{E}_0 & \xrightarrow{\widehat{\Sigma}_0} & \mathcal{E}_1 & \xrightarrow{\widehat{\Sigma}_1} & \cdots & \longrightarrow & \mathcal{E}_{d-1} & \xrightarrow{\widehat{\Sigma}_{d-1}} & \mathcal{E}_0 \\
\downarrow{\scriptstyle\pi} & & \downarrow{\scriptstyle\pi} & & & & {\scriptstyle\pi}\downarrow & & {\scriptstyle\pi}\downarrow \\
E_0 & \xrightarrow{\widehat{\sigma}_0} & E_1 & \xrightarrow{\widehat{\sigma}_1} & \cdots & \longrightarrow & E_{d-1} & \xrightarrow{\widehat{\sigma}_{d-1}} & E_0
\end{array}$$

及

$$\begin{array}{ccc} \mathcal{E} & \xrightarrow{\widehat{\mathcal{F}}} & \mathcal{E} \\ \downarrow \pi & & \downarrow \pi \\ E & \xrightarrow{\widehat{F}} & E \end{array}$$

其中 $\widehat{\sigma}_i$ 是 σ_i 的对偶同种, $\widehat{\Sigma}_i$ 是 Σ_i 的对偶同种等等.

Satoh 算法由两方面组成：提升所有需要的信息到 $\mathbb{Z}_q$(足够的精度), 然后借助这些提升的数据找出 Frobenius 的迹, 我们给出其大意：

(算法 10.2) Procedure Satoh Alorithm

Inputs: 椭圆曲线 $E/\mathbb{F}_q$, 使 $j = j(E) \notin \mathbb{F}_{p^2}$.

Output: E 的 Frobenius 迹.

1. 计算曲线 E_i 和其 j 不变量 j_i 的闭链, $0 \leqslant i \leqslant d-1$;
2. 提升 j 不变量, 曲线的系数及其 p-torsion 点子群;
3. 计算迹.

下面分别讨论这些问题：

(1) 提升：我们将应用 $\mathbb{F}_q$ 中的 σ 构造 j 不变量的闭链, 然后利用一个多变量的牛顿迭代同时提升所有这些 j 不变量, 利用这种方法, 能得到所有共轭的 $J\,(\in \mathbb{Z}_q)$ 而不必计算 Σ. 一旦如此, 则我们可以利用牛顿迭代提升所有曲线 (只要提升它们的系数即可), 关于这个提升, 参见上节命题 9.1. 同种 $\widehat{\sigma}_i$ 和 $\widehat{\Sigma}_i$ 是次数为 p 的可分映射, 故它们由其核 (具有阶 p) 决定, 因此通过提升椭圆曲线的 p-torsion 点子群, 就可以提升 $\widehat{\sigma}$ 和 $\widehat{\Sigma}_i$, 参见定理9.2. 而为了提升 p-torsion 子群, 我们只要利用牛顿迭代提升一个点 (若 $p=2$ 或 3), 或提升 p 除子多项式的一个因子 ($p \geqslant 5$) 即可.

(算法 10.3) Procedure Satoh Lift

Inputs: 一个定义在 $\mathbb{F}_q$ 上的椭圆曲线 E_i 的闭链.

Output: 一个定义在 $\mathbb{Z}_q$ 上的椭圆曲线 $\mathcal{E}_i$ 的闭链：

$$\mathcal{E}_0 \to \mathcal{E}_1 \to \cdots \to \mathcal{E}_{d-1} \to \mathcal{E}_0$$

及其 p-torsion 子群.

1. 计算 d 条椭圆曲线 E_i 及其 j 不变量 j_i 的闭链;
2. 同时提升所有 j_i, 得出 J_i;

3. 通过提升系数而提升每一条椭圆曲线;
4. 提升每一条椭圆曲线的 p-torsion 子群.

---

(2) 计算迹：目的是计算 Frobenius $F:\ E \to E$ 的迹. 假设我们已经计算了曲线 $\mathcal{E}$(在一个好精度下), 它是 E 的典范提升, 具有性质 $\operatorname{Tr} F = \operatorname{Tr} \mathcal{F}$. 此处 $\mathcal{F}$ 是在 $\mathcal{E}$ 上的 Frobenius. 由一个自同态的迹等于其对偶的迹, 故只要计算其对偶 $\widehat{F}$ 的迹

$$\operatorname{Tr} F = \operatorname{Tr} \mathcal{F} = \operatorname{Tr} \widehat{\mathcal{F}},$$

但 F 可分解为 “小 Frobenius” 之积, 故

$$\operatorname{Tr} \mathcal{F} = \operatorname{Tr}\left(\widehat{\Sigma}_{d-1} \circ \widehat{\Sigma}_{d-2} \circ \cdots \circ \widehat{\Sigma}_0\right).$$

然后过渡到形式群, 正如上节命题9.2所述：记 τ 是 $\mathcal{E}$ 的局部参数 $-X/Y$, τ_i 是 $\mathcal{E}_i$ 的局部参数, 设 $\widehat{\mathcal{F}}(\tau) = \sum_{k\geqslant 1} c_k \tau^k$, 则

$$\operatorname{Tr} \mathcal{F} = \operatorname{Tr}\left(\widehat{\mathcal{F}}(\tau)\right) = c_1 + \frac{q}{c_1}.$$

故为了计算迹, 只要算出第 1 个系数 c_1 即可. 但如果写 $\widehat{\Sigma}_i:\ \mathcal{E}_i \to \mathcal{E}_{i+1}$ 伴随的形式群同态为 $\widehat{\Sigma}_i(\tau_i) = g_i \tau_{i+1} + O\left(\tau_{i+1}^2\right)$, 则 $c_1 = \prod_{0\leqslant i<d} g_i$, 于是

$$\operatorname{Tr} F \equiv \prod_{0\leqslant i<d} g_i \pmod q.$$

注意到这些 g_i 之积是 g_0 从 $\mathbb{Z}_q$ 到 $\mathbb{Z}_p$ 的范数 (Norm) 的一个表达式, 即：$\prod_{0\leqslant i<d} g_i = \mathrm{Norm}_{\mathbb{Z}_q/\mathbb{Z}_p}(g_0)$, 因此它肯定是在 $\mathbb{Z}_p$ 中的.

最后一步就是从曲线 $\mathcal{E}_i$ 和 $\mathcal{E}_{i+1}$ 及 $\widehat{\Sigma}_i$ 的核计算 g_i, 这可借助于 Vélu 公式进行, 正如上一章命题9.4中所述.

§10.3　提升的算法

一、椭圆曲线闭链的提升

Deuring, Lubin, Serre 和 Tate 的定理保证了我们想构造的 J_i 的链由

$$\Phi_p(J_i, J_{i+1}) = 0,\ 0 \leqslant i < d$$

所刻画. 从 j_i 计算 J_i 的算法由上一章的命题9.1给出：它是基于作用在 d 维向量空间上的下述函数的牛顿迭代：

$$\Theta(x_0, \cdots, x_{d-1}) = \left(\Phi_p(x_0, x_1), \Phi_p(x_1, x_2), \cdots, \Phi_p(x_{d-2}, x_{d-1}), \Phi_p(x_{d-1}, x_0)\right),$$

此时，我们必须考虑该函数的 Jacobian 矩阵

$$D\Theta(x_0,\cdots,x_{d-1})=\begin{pmatrix}\Phi_p'(x_0,x_1) & \Phi_p'(x_1,x_0) & 0 & \cdots & 0\\ 0 & \Phi_p'(x_1,x_2) & \Phi_p'(x_2,x_1) & \cdots & 0\\ 0 & 0 & 0 & \cdots & \Phi_p'(x_{d-1},x_{d-2})\\ \Phi_p'(x_0,x_{d-1}) & 0 & 0 & \cdots & \Phi_p'(x_{d-1},x_0)\end{pmatrix},$$

此处 $\Phi_p'(X,Y)$ 记 $\Phi_p(X,Y)$ 关于 X 的偏导数. 而迭代本质上是

$$(x_0,\cdots,x_{d-1})\longleftarrow(x_0,\cdots,x_{d-1})-\big((D\Theta)^{-1}\Theta\big)(x_0,\cdots,x_{d-1}).$$

(算法 10.4) Procedure Lift J Invariants

Inputs: 一个期望的精度 n 及一条闭链 $j_i\in\mathbb{F}_q\setminus\mathbb{F}_{p^2}$, 使得 $\Phi_p(j_i,j_{i+1})\equiv 0\pmod p$, $0\leqslant i<d$.

Output: 一条定义在 $\mathbb{Z}_q$ 上的椭圆曲线 $\mathcal{E}_i$ 的闭链的 j 不变量.

1. 若 $n=1$ 则选择任意的 J_i, 使得 $\pi(J_i)=j_i$, goto 5;
2. $n'\longleftarrow[\frac{n}{2}]$;
3. $(J_0,J_1,\cdots,J_{d-1})\longleftarrow$Lift J Invariants $\big((j_0,j_1,\cdots,j_{d-1}),n'\big)$;
4. $(J_0,J_1,\cdots,J_{d-1})\longleftarrow$Update $J_s\big((J_0,J_1,\cdots,J_{d-1}),n\big)$;
5. Return $(J_0,J_1,\cdots,J_{d-1})$.

(算法 10.5) Procedure Update J_s

Inputs: 一个期望的精度 n 及一条闭链 $J_i\in\mathbb{Z}_q$, 使得

$$\Phi_p(J_i,J_{i+1})\equiv 0\pmod{p^{[n/2]}},\quad 0\leqslant i<d.$$

Output: 一条闭链 $\mathfrak{J}_i\in\mathbb{Z}_q$, 使得 $\Phi_p(\mathfrak{J}_i,\mathfrak{J}_{i+1})\equiv 0\pmod{p^n}$ 且

$$\mathfrak{J}_i\equiv J_i\pmod{p^{[n/2]}},\quad 0\leqslant i<d.$$

1. Allocate arrays $D[0,\cdots,d-2], P[0,\cdots,d-1]$ and $\mathfrak{J}[0,\cdots,d-1]$ of elements of $\mathbb{Z}_q$;
2. For i=0 to $d-2$, do

   2.1 $t\longleftarrow 1/\Phi'(J_i,J_{i+1})$;

2.2 $D_i \longleftarrow t \cdot \Phi'(J_{i+1}, J_i)$;

2.3 $P_i \longleftarrow t \cdot \Phi'(J_i, J_{i+1})$;

3. $m \longleftarrow \Phi'(J_0, J_{d-1})$;

4. $f \longleftarrow \Phi'(J_{d-1}, J_0)$;

5. For $i = 0$ to $d-2$ do

5.1 $f \longleftarrow f - m \cdot P_i$;

5.2 $m \longleftarrow -m \cdot D_i$;

5.3 If $m \equiv 0 \pmod{p^n}$ Then break;

6. $m \longleftarrow m + \Phi'(J_{d-1}, J_0)$;

7. $f \longleftarrow f/m$;

8. $P_{d-1} \longleftarrow f$;

9. For $i = d-2$ down to 0 do

9.1 $P_i \longleftarrow P_i - D_i \cdot P_{i+1}$;

10. For $i = 0$ to $d-2$ do

10.1 $\mathfrak{J}_i \longleftarrow J_i - P_i$;

11. $\mathfrak{J}_{d-1} \longleftarrow J_{d-1} - f$;

12. Free arrays D and P;

13. Return $(\mathfrak{J}_0, \mathfrak{J}_1, \cdots, \mathfrak{J}_{d-1})$.

二、提升曲线的方程

现设 $p \geqslant 5$. 于是 $E/\mathbb{F}_q$ 的 Weierstrass 方程可选取具有形式

$$y^2 = x^3 + ax + b.$$

我们想提升 E 到一条椭圆曲线 $\mathcal{E}/\mathbb{Z}_q$:

$$Y^2 = X^3 + AX + B.$$

其 j 不变量已知. 为此, 我们可以任意提升其中一个系数, 然后利用牛顿迭代提升另一个系数, 牛顿迭代基于以下方程:

$$J = -1728\frac{(4A)^3}{\Delta},$$

其中 $\Delta = -16(4A^3 + 27B^2)$. 因 $p \geqslant 5$ 且 $J \notin \mathbb{F}_{p^2}$ 保证了迭代中的分母不为零. 因此每次迭代精度增长 1 倍.

(算法 10.6) Procedure Lift A And B

Inputs: 一个 j 不变量 $J \in \mathbb{Z}_q$, 椭圆曲线 $E/\mathbb{F}_q$ 的系数 a 和 b 及其 j 不变量 $\pi(J)$, 一个期望的精度 n.

Output: 一条椭圆曲线 $\mathcal{E}/\mathbb{Z}_q$ 的系数 $A, B \in \mathbb{Z}_q$, 使得 $j(\mathcal{E}) = J$, 提升精度 (对 A, B) 为 n.

1. 任意选取 $A \in \mathbb{Z}_q$, 使得 $\pi(A) = a$;
2. $B \longleftarrow$ **LiftBGivenA**(J, A, b, n);
3. Return A, B.

(算法 10.7) Procedure LiftBGivenA

Inputs: 一个 j 不变量 J 及一个系数 $A \in \mathbb{Z}_q$, 一个系数 $b \in \mathbb{F}_q$, 期望的精度 n.

Output: 一个系数 $B \in \mathbb{Z}_q$, 提升到精度 n.

1. 若 $n = 1$, 则任意选取 $B \in \mathbb{Z}_q$, 使得 $\pi(B) = b$; goto 5;
2. $n' \longleftarrow [\frac{n}{2}]$;
3. $B \longleftarrow$ **LiftBGivenA**(J, A, b, n');
4. $B \longleftarrow B - \frac{J(4A^3+27B^2)-6912A^3}{54JB}$ (到精度 n);
5. Return B.

三、提升 p-torsion 子群

在 Satoh 算法中, 提升 p-torsion 子群是更为精细的工作, 主要想法是通过提升 E_i 的 p 除子多项式 $\psi_p(x)$ 的一个因子. 这里有两个问题出现:

- 提升一个因子不像提升一个根那样简单;
- $\psi_p(x)$ 的导数 mod p 后为零, 所以在精度方面要小心, 特别检查初始要求的精度十分重要.

该算法的基础是上一章中的引理9.1. 现在重述其特例如下:

定理 10.2 设 $\Psi(x)$ 是 p-adic 域上一个多项式, $p \| \Psi'(x)$, $h(x)$ 是已知精度为 n 的首一多项式且

- $\pi\big(h(x)\big)$ 无平方因子且与 $\pi\big(p^{-1}\Psi'(x)\big)$ 互素,
- $h(x)$ 整除 $\Psi(x)$ 到精度 $n+1$.

定义一个新的多项式

$$\mathfrak{h}(x) = h(x) + \left(\frac{\Psi(x)}{\Psi'(x)} h'(x) \pmod{h(x)}\right),$$

则 $\mathfrak{h}(x)$ 有以下性质:

- $h(x) \equiv \mathfrak{h}(x) \pmod{p^2}$,
- $h(x)$ 整除 $\Psi(x)$ 到精度 $2n+1$.

更进一步, 若 $n \geqslant 1$, 则 $\pi\big(h(x)\big) = \pi\big(\mathfrak{h}(x)\big)$, 且上述过程是可以重复的.

(算法 10.8) Procedure Lift H

Inputs: 一椭圆曲线 $E_{i+1}/\mathbb{F}_q$, 一椭圆曲线 $\mathcal{E}_i/\mathbb{Z}_q$ 及期望的精度 n.

Output: $\mathcal{E}_i$ 的 p 除子多项式的一个首 1 因子 $H(x)$, 表示 $\widehat{\Sigma}_i$ 的核.

1. $\Phi(x) \longleftarrow \mathcal{E}_i$ 的 p 次除子多项式 (其次数为 $\frac{p^2-1}{2}$);
2. $\psi(x) \longleftarrow E_{i+1}$ 的 p 次除子多项式 (它是一个次数 $\frac{p-1}{2}$ 的多项式 $h(x)$ 的 p 次幂);
3. $h(x) \longleftarrow 0$;
4. For $k=0$ to $\frac{p-1}{2}$ do

   4.1 $h(x) \longleftarrow h(x) + \frac{u_k}{u_{(p-1)/2}} x^k$, u_k 是 $\psi(x)$ 的 x^{pk} 的系数;
5. $H(x) \longleftarrow$**LiftHbis**$\big(\Psi(x), h(x), n\big)$;
6. Return $H(x)$.

(算法 10.9) Procedure LiftHbis

Inputs: 一多项式 $\Psi(x)$, 一个近似值 $h(x)$ 及期望的精度 n.

Output: $\Psi(x)$ 的一个首 1 因子 $H(x)$(精度到 n).

1. 若 $n=1$, 则 $H(x) \longleftarrow h(x)$, goto 5;
2. $n' \longleftarrow [\frac{n-1}{2}]$;
3. $H(x) \longleftarrow$ **LiftHbis**$\big(\Psi(x), h(x), n'\big)$;
4. $H(x) \longleftarrow H(x) - (\frac{\Psi(x)}{\Psi'(x)} H'(x) \pmod{H(x)})$(到精度 n);
5. Return $H(x)$.

四、特征 2 的情形

众所周知, 对于特征 2 的有限域上的椭圆曲线 E, 总可以找到 E 的一个方程 (或 E 的 twist 的方程) 具有形式

$$y^2 + xy = x^3 + a,$$

因此, 我们将只讨论这种情形的方程.

提升曲线的方程的算法就是利用牛顿迭代提升其系数 a, 从而得出方程

$$\mathcal{E}: \quad y^2 + xy = x^3 + A$$

的系数 A. 因为 $J = \frac{1}{\Delta}$, $\Delta = -A - 432A^2$ 是 $\mathcal{E}$ 的判别式, 故我们要计算其根的多项式是 $f(x) = 1 + J\big(x + 432x^2\big)$, 而初始值是 $-1/J \pmod{16}$.

在这种情形下, 每一步迭代精度增长是从 n 到 $2n+4$. 设 x 是精度 n 的一个近似值, 设 e 是精度 n 时的误差项, 即 $e = f(x)$, 而 y 是下一步的近似值, 即 $y = x - e/e'$, 其中 $e' = J\big(1 + 864x\big)$ 是 $f'(x)$. 于是在这一步的误差项是

$$f(y) = 1 + J\big(y + 432y^2\big) = 432J\frac{e^2}{e'^2}.$$

我们有 $e = O(2^n)$, $2 \nmid e'$ 且 $2^4 \| 432$, 故 $f(y) = O\big(2^{2n+4}\big)$.

(算法 10.10) Procedure Lift A

Inputs: 一条椭圆曲线 $\mathcal{E}/\mathbb{Z}_q$ 的 j 不变量 J 及期望的精度 n.

Output: 被提升的曲线 $\mathcal{E}/\mathbb{Z}_q$ 的系数 A, 精度为 n.

1. 若 $n \leqslant 4$, 则 $A \longleftarrow -1/J$; goto 5;
2. $n' \longleftarrow [\frac{n-4}{2}]$;
3. $A \longleftarrow$**LiftA**(J, n');
4. $A \longleftarrow A - \frac{1+J(A+432A^2)}{J(1+864A)}$(到精度 n);
5. Return A.

下面讨论提升 2-torsion 点, 算法的思想是类似的, 此时, 用在牛顿迭代中的函数 $f(x)$ 是被提升了的曲线 $\mathcal{E}$ 上非平凡 2-torsion 点的横坐标所满足的方程, 即 2 除子多项式 $4X^3 + X^2 + 4A$. 这个方程的根模 2 必定为 0. 置 $X = 2Z$, 我们得出改进的除子多项式 $8Z^3 + Z^2 + A$. 此时, 应用基于函数 $f(x) = 8x^3 + x^2 + A$ 的牛顿迭代提升 Z, 初始近似值是 $1/\sqrt{J} \pmod 8$. 注意, 并不必计算 $\sqrt{J} \pmod 8$, 因为我们已经计算了整个提升曲线的闭链, 且因 $J = j(\mathcal{E}_i)$, 故有 $\sqrt{J} = j(\mathcal{E}_{i+1}) \pmod 8$(这可利用 $\Phi_2(X,Y)$ 得出, 因 $\Phi_2\big(j(\mathcal{E}_i), j(\mathcal{E}_{i+1})\big) = 0$, 故

$$\Phi_2\big(J, j(\mathcal{E}_{i+1})\big) \equiv 0 \pmod 8.$$

由 Φ_2 的具体方程知上式即是

$$\big(J^2 - j(\mathcal{E}_{i+1})\big)\big(J - j(\mathcal{E}_{i+1})^2\big) \equiv 0 \pmod 8,$$

此时, 在每一步迭代时, 精度从 n 增加到 $2n-2$: 设 x 是精度 n 的近似值, e 是误差项, 即 $e=f(x)$, 设 y 是下一步的近似值, 即 $y=x-e/e'$, $e'=2(12x^2+x)$, 则这一步的误差项是

$$f(y)=8y^3+y^2+A=\frac{e^2}{e'^2}(24x+1)-8\frac{e^3}{e'^3},$$

而 $e=O(2^n)$, $2\|e'$, 故 $f(y)=O\big(2^{\min(2n-2,3n)}\big)=O\big(2^{2n-2}\big)$.

(算法 10.11) Procedure Lift Z

Inputs: j 不变量 J, $\mathcal{E}/\mathbb{Z}_q$ 的系数 A 及其期望的精度 n.

Output: 已提升曲线 $\mathcal{E}/\mathbb{Z}_q$ 的 Z, 精度为 n.

1. 若 $n\leqslant 3$, 则 $Z\longleftarrow 1/\sqrt{J}$; goto 5;
2. $n'\longleftarrow [\frac{n+2}{2}]$;
3. $Z\longleftarrow$**LiftZ**(J,A,n');
4. $Z\longleftarrow Z-\frac{8Z^3+Z^2+A}{2(12Z^2+Z)}$ 到精度 n;
5. Return Z.

---

§10.4 计 算 迹

由上节我们知道, Vélu 的公式给出了从 $\mathcal{E}_i$ 到 $\mathcal{E}_{i+1}$ 的 “小 Verschiebung” 的第一个系数的简单表达式, 而计算 Frobenius 的迹就是求所有这些表达式之积.

设 E 是一椭圆曲线, F 是 E 的有限子群, 则 E/F 同构于一椭圆曲线. Vélu 的公式给出了一椭圆曲线 $E'(\simeq E/F)$ 的清晰的方程, 以及从 E 到 E' 的同种的清晰的公式, 而且这个同种如果以形式群的同态的形式写出, 其第一个系数是 1.

现在将它应用到我们的问题: 已有两曲线 $\mathcal{E}_i$ 和 $\mathcal{E}_{i+1}$ 以及 $\mathcal{E}_i$ 的一个子群, 想知道从 $\mathcal{E}_i$ 到 $\mathcal{E}_{i+1}$ 的对应该核的同种在形式群表示下的第一个系数.

第 1 步是利用 Vélu 公式(参见文献 [13]) 计算曲线 $\mathcal{E}_i'$, 则 $\mathcal{E}_i'$ 和 $\mathcal{E}_{i+1}$ 同构, 我们可以清晰计算这个同构 λ 以及它在形式群表示下的第一个系数, 总之, 我们有图 10.1:

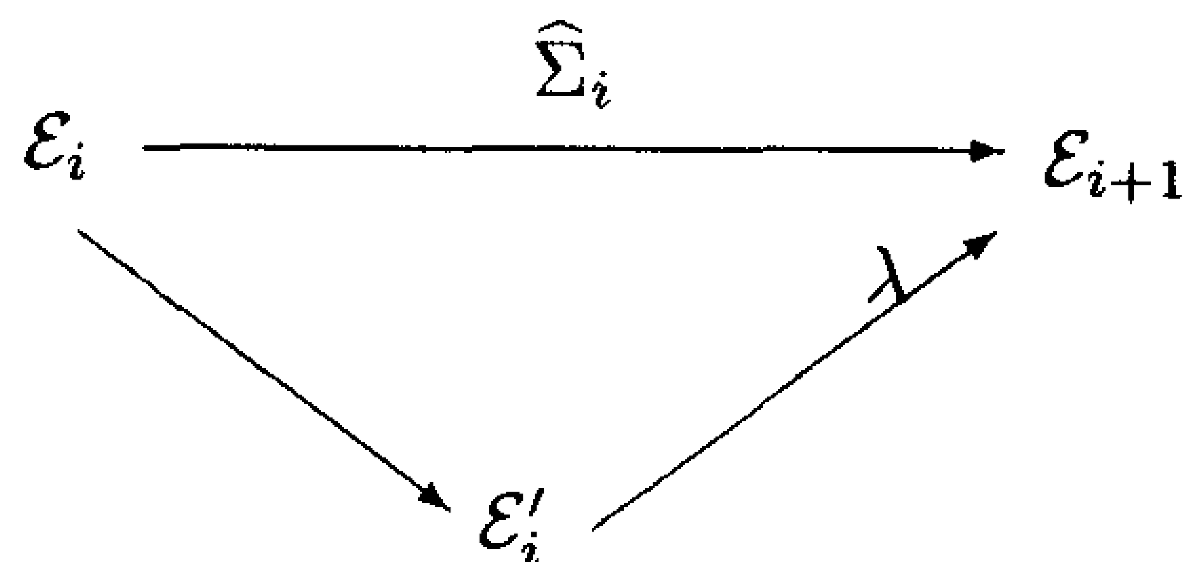


图 10.1

于是同种 $\widehat{\Sigma}_i$ 的第一个系数等于 Vélu 同种的第一个系数 (它等于 1) 和同构 λ 的第一个系数之积, 具体如下:

(1) 特征 $p \geqslant 5$ 的情形

$\mathcal{E}_i$ 的方程具有形式

$$\mathcal{E}_i: \ y^2 = x^3 + A_i x + B_i,$$

$\mathcal{E}_{i+1}$ 的方程具有形式

$$\mathcal{E}_{i+1}: \ y^2 = x^3 + A_{i+1} x + B_{i+1}.$$

$\widehat{\Sigma}_i$ 的核由 $\mathcal{E}_i$ 的无穷远点和 $p-1$ 个有限点 (它们的 $\frac{p-1}{2}$ 个横坐标由多项式 $H_i(x)$ 的根给出) 组成. $\mathcal{E}_i'$ 的方程由 Vélu 公式 (参见文献 [13]) 给出:

$$\begin{aligned}
\mathcal{E}_i': \ & y^2 = x^3 + \alpha_i x + \beta_i, \\
& \alpha_i = (6-5p)A_i - 30(s_1^2 - 2s_2), \\
& \beta_i = (15-14p)B_i - 70(-s_1^3 + 3s_1 s_2 - 3s_3) + 42A_i s_1,
\end{aligned}$$

其中 s_k 记 $H_i(x)$ 的 $x^{\frac{p-1}{2}-k}$ 的系数.

由于 $\mathcal{E}_i' \simeq \mathcal{E}_{i+1}$, 于是存在同构 $\lambda: \mathcal{E}_i' \to \mathcal{E}_{i+1}$, 从而存在 g_i, 使得

$$\lambda(x, y) = (g_i^2 x, g_i^3 y),$$

其中 g_i 是我们要求的项, 但

$$B_{i+1} = \beta_i g_i^6, \quad A_{i+1} = \alpha_i g_i^4,$$

所以

$$g_i^{-2} = \frac{\beta_i}{\alpha_i} \cdot \frac{A_{i+1}}{B_{i+1}}.$$

于是形式群上 $\widehat{\Sigma}_i$ 的第 1 个系数等于 λ 在形式群上第 1 个系数 $1/g_i$, $\widehat{\Sigma}_i$ 的第 1 个系数等于 $\sqrt{\frac{\beta_i}{\alpha_i} \cdot \frac{A_{i+1}}{B_{i+1}}}$.

(算法 10.12) Procedure Compute Trace char p

Inputs: 一椭圆曲线 $E/\mathbb{F}_{p^d}: \ y^2 = x^3 + ax + b$, $j(E) \notin \mathbb{F}_{p^2}$.

Output: Frobenius 的迹.

1. $n \longleftarrow [\log_p 4 + \frac{d}{2}]$;

2. $(j_i), (a_i), (b_i)$, $0 \leqslant i < d \longleftarrow j(E), a, b$ 的共轭;

3. $(J_i), 0 \leqslant i < d \longleftarrow$**Lift** J **invariants**$((j_i), n)$;
4. $N \longleftarrow 1$; $D \longleftarrow 1$;
5. For $i = 0$ to $d-1$ do
   5.1 $A, B \longleftarrow$**Lift A and B**(J_i, a, b, n);
   5.2 $H \longleftarrow$**Lift H**$(a_{i+1}, b_{i+1}, A, B, n)$;
   5.3 $s_1, s_2, s_3 \longleftarrow H(x)$ 中 $x^{\frac{p-1}{2}-1}, x^{\frac{p-1}{2}-2}, x^{\frac{p-1}{2}-3}$ 的系数;
   5.4 $\alpha \longleftarrow (6-5p)A - 30(s_1^2 - 2s_2)$;
   5.5 $\beta \longleftarrow (15-14p)B - 70(-s_1^3 + 3s_1s_2 - 3s_3) + 42As_1$;
   5.6 $N \longleftarrow N\beta A$;
   5.7 $D \longleftarrow D\alpha B$;
6. $c \longleftarrow \sqrt{N/D}$ 到精度 n;
7. $h_E \longleftarrow E$ 的 Hasse 不变量;
8. 若 $c \not\equiv h_E \pmod p$, 则 $c \longleftarrow -c$;
9. 约化 c 到一个在 $0, 1, \cdots, p^n$ 中的整数. 若 $c > 2\sqrt{q}$, 则 $c \longleftarrow c - p^n$;
10. Return c.

注意: (a) 在第 6 步中, 可用牛顿迭代求平方根;

(b) $E:\ y^2 = x^3 + ax + b$ 的 Hasse 不变量定义为多项式 $(x^3+ax+b)^{(p-1)/2}$ 中 x^{p-1} 的系数的范 (Norm).

(c) 关于第 8 步的理由如下: 由于第 6 步中求出一个平方根 c 后, 另一个平方根就是 $-c$, 于是需要确定这 2 个平方根中哪一个是我们的椭圆曲线的 Frobenius 的迹. 但是如果记 E 的 Hasse 不变量为 h_E, 则有

$$\#E(\mathbb{F}_q) = q + 1 - t = 1 - h_E \qquad (\text{作为 } \mathbb{F}_q \text{ 中元素}),$$

于是 mod p 知应有

$$t \equiv h_E \pmod p,$$

其中 $t = \operatorname{Tr} Fr_q$.

(2) 特征 $p = 2$ 的情形

$$\mathcal{E}_i:\ y^2 + xy = x^3 + A_i; \qquad \mathcal{E}_{i+1}:\ y^2 + xy = x^3 + A_{i+1}.$$

在特征 2 时, $\widehat{\Sigma}_i$ 的核之阶为 2, 它是 $\mathcal{E}_i$ 的子群, 设 (X_i, Y_i) 是该子群的非平凡点, 由 Vélu 公式给出的椭圆曲线 $\mathcal{E}_i'$ 的方程式为

$$y^2 + xy = x^3 + \mathcal{A}_4 x + \mathcal{A}_6,$$

其中

$$\mathcal{A}_4 = -5t, \quad \mathcal{A}_6 = A_i - t - 7w,$$
$$t = 3X_i^2 - Y_i, \quad w = X_i t.$$

与特征不小于 5 的情形类似, 有了 $\mathcal{E}_i'$ 和 $\mathcal{E}_{i+1}$ 的方程后, 就可以计算同构 $\lambda: \mathcal{E}_i' \simeq \mathcal{E}_{i+1}$, 从而可求出系数 g_i^2. 在进行坐标平移后 (这并不影响该同构的形式群表示的第一个系数), 有

$$\mathcal{E}_{i+1}: \ y^2 = x^3 - \frac{1}{48}x + \frac{1}{864} + A_{i+1},$$
$$\mathcal{E}_i': \ y^2 = x^3 + \left(\mathcal{A}_4 - \frac{1}{48}\right)x + \frac{1}{864} + \mathcal{A}_6 - \frac{\mathcal{A}_4}{12},$$

从而

$$g_i^{-2} = \frac{-\frac{1}{48}}{\frac{1}{864} + A_{i+1}} \cdot \frac{\frac{1}{864} + \mathcal{A}_6 - \frac{\mathcal{A}_4}{12}}{\mathcal{A}_4 - \frac{1}{48}} = \frac{72\mathcal{A}_4 - 1 - 864\mathcal{A}_6}{(48\mathcal{A}_4 - 1)(1 + 864A_{i+1})}.$$

将上述各项用 A_i 和 X_i 表示出来 (注意 $Y_i = -\frac{X_i}{2}$), 有

$$\begin{aligned} g_i^{-2} &= -\frac{-18144X_i^3 - 4536X_i^2 - 252X_i + 1 + 864A_i}{(720X_i^2 + 120X_i + 1)(1 + 864A_{i+1})} \\ &= \frac{1 - 252X_i + 19008A_i}{\left(1 + 120(X_i + 6X_i^2)\right)(1 + 864A_{i+1})}. \end{aligned}$$

此处用到了 $4X_i^3 + X_i^2 + 4A_i = 0$(2 除子多项式).

回忆前面提升的是 $Z_i = X_i/2$, 而不是 X_i, 又对于计算 2-adic 平方根时, 需要多一比特的精度, 于是有算法如下:

(算法 10.13) Procedure Compute Trace char 2

Inputs: 一椭圆曲线 $E/\mathbb{F}_{2^d}: \ y^2 + xy = x^3 + a$, $j(E) \notin \mathbb{F}_4$.

Output: $E/\mathbb{F}_{2^d}$ 的 Frobenius 的迹.

1. $n \longleftarrow [\frac{d+6}{2}]$;
2. $(j_i) 0 \leqslant i < d \longleftarrow j(E)$ 的共轭;
3. (J_i), $0 \leqslant i < d$ ⟵**Lift** J **invariants**$((j_i), n)$;
4. $N \longleftarrow 1$; $D \longleftarrow 1$;
5. For $i = 0$ to $d - 1$ do
   5.1 A ⟵**LiftA**(J_i, n);
   5.2 Z ⟵**LiftZ**(J_i, A, n);

5.3 $A \longleftarrow 864A$;

5.4 $N \longleftarrow N(1-504Z+22A)$;

5.5 $D \longleftarrow D(1+240(Z+12Z^2))(1+A)$;

6. $c \longleftarrow \sqrt{N/D}$ 到精度 n;

7. 若 $c \not\equiv 1 \pmod 4$, 则 $c \longleftarrow -c$;

8. 约化 c 到一个在 $0,1,\cdots,2^{n-1}$ 中的整数. 若 $c > 2\sqrt{q}$, 则 $c \longleftarrow c-2^{n-1}$;

9. Return c.

(3) 特征 3 的情形

在特征 3 时, 一椭圆曲线的方程 (j 不变量 $\neq 0$) 为

$$E: \ y^2 = x^3 + a_2x^2 + a_6,$$

此时, $j(E) = -a_2^3/a_6$, 提升后的曲线 $\mathcal{E}$ 具有形式

$$\mathcal{E}: \ y^2 = x^3 + A_2x^2 + A_6,$$

其 j 不变量为 $J = -256A_2^6/(4A_2^3A_6 + 27A_6^2)$.

因此为了提升曲线的系数, 我们可以应用与 char $p \geqslant 5$ 时几乎完全相同的算法, 即: 先任意提升系数 A_2, 然后应用基于函数 $f(x) = J(A_2^3x + \frac{27}{4}x^2) + 64A_2^6$ 的牛顿迭代提升 A_6, 初始值 $x_0 = a_6$.

而为了提升 3-torsion 子群, 只要提升一个非平凡的 3-torsion 点即可, $\mathcal{E}$ 的 3 除子多项式是 $\Psi_3(x) = 3x^4 + 4A_2x^3 + 12A_6x + 4A_2A_6$, 而 E 的 3 除子多项式是 $\psi(x) = a_2(x^3 + a_6)$. 我们可以应用基于函数 $\Psi_3(x)$ 的牛顿迭代来提升 3-torsion 子群, 初始值是 $x_0 = -\sqrt[3]{A_6}$, 此时迭代是有效的, 因为我们有

$$\Psi_3(x_0) = -3A_6x_0 - 4A_2A_6 + 12A_6x_0 + 4A_2A_6 = 9A_6x_0,$$
$$\Psi_3'(x_0) = -12A_6 + 12A_2x_0^2 + 12A_6 = 12A_2x_0^2,$$

故 $\Psi_3(x_0) \equiv 0 \pmod 9$, $\Psi'(x_0) \equiv 0 \pmod 3$, 但 $\Psi'(x_0) \not\equiv 0 \pmod 9$(注意 $A_2 \neq 0$ 且 $A_6 \neq 0$).

对于迹的计算, 方法类似于特征 2 时的情形, 但此时曲线的方程形式和 Vélu 公式的形式有所不同, 设

$$y^2 = x^3 + A_ix^2 + B_i.$$

记 X_i 是被提升后的 3-torsion 点的 x 坐标, 则 Vélu 公式给出

$$\mathcal{E}_i': \ y^2 = x^3 + a_2x^2 + a_3x + a_6,$$

其中

$$a_2 = A_i, \quad a_4 = -5t, \quad a_6 = B_i - 4A_it - 7w,$$

$$t = 6X_i^2 + 4A_iX_i, \quad w = 10X_i^3 + 8A_iX_i^2 + 4B_i.$$

现在通过坐标平移变换后, $\mathcal{E}_i'$ 和 $\mathcal{E}_{i+1}$ 的方程变为

$$\mathcal{E}_{i+1}: y = x^3 - \frac{1}{3}A_{i+1}^2 x + B_i + \frac{2}{27}A_{i+1}^3,$$

$$\mathcal{E}_i': y = x^3 + \left(a_4 - \frac{1}{3}a_2^2\right)x + a_6 + \frac{2}{27}a_2^3 - \frac{1}{3}a_2a_4,$$

由此可以很容易地与前面类似推出 g_i^{-2} 的表达式

$$g_i^{-2} = \frac{A_{i+1}^2\big(-1890X_i^3 - 1890A_iX_i^2 - 252A_i^2X_i + 2A_i^3 - 729B_i\big)}{\big(2A_{i+1}^3 + 27B_i\big)\big(90X_i^2 + 60A_iX_i + A_i^2\big)}.$$

最后的迹就是

$$\operatorname{Tr} Fr_q = \prod_{0 \leqslant i < d} g_i^{-1} \pmod q.$$

基于此, 我们可以与特征 2 类似写出有关算法.

第十一章　Mestre 的 AGM 算法

§11.1　典范提升的 j 不变量的计算

对于实数 $a_0, b_0 \in \mathbb{R}$, $a_0 \geqslant b_0 > 0$, 定义算术几何平均迭代如下：

$$(a_{k+1}, b_{k+1}) = \left(\frac{a_k + b_k}{2}, \sqrt{a_k b_k}\right) \qquad k \geqslant 1,$$

则 $b_k \leqslant b_{k+1} \leqslant a_{k+1} \leqslant a_k$, 且 $0 \leqslant a_{k+1} - b_{k+1} \leqslant (a_k - b_k)/2$, 所以有极限存在：

$$\lim_{k\to\infty} a_k = \lim_{k\to\infty} b_k.$$

这个极限称为 a_0 和 b_0 的算术几何平均 (简称为 AGM), 记为 $AGM(a_0, b_0)$. 计算表明

$$\frac{a_k}{b_k} - 1 \leqslant \frac{a_0 - b_0}{2^k b_k} \leqslant \frac{1}{2^k}\left(\frac{a_0}{b_0} - 1\right).$$

因此, 经过对数多个步骤后, 有 $a_k/b_k = 1 + \varepsilon_k$, $\varepsilon_k < 1$. 而 $(1+\varepsilon_k)^{-1/2}$ 的泰勒展开式表明收敛性是 2 次的：

$$\frac{a_{k+1}}{b_{k+1}} = \frac{a_k + b_k}{2\sqrt{a_k b_k}} = \frac{2 + \varepsilon_k}{2\sqrt{1+\varepsilon_k}} = 1 + \frac{\varepsilon_k^2}{8} - \frac{\varepsilon_k^3}{8} + \frac{15\varepsilon_k^4}{128} - \frac{7\varepsilon_k^5}{64} + O(\varepsilon_k^6), \tag{11.1}$$

现在设 $\mathbb{Q}_q$ 是 $\mathbb{Q}_2$ 的 n 次非分歧扩张, $\mathbb{Z}_q$ 是 $\mathbb{Q}_q$ 的赋值环, $\mathbb{F}_q$ 是 $\mathbb{Q}_q$ 的剩余类域. 对于 $c \in 1 + 8\mathbb{Z}_q$, 令 $\sqrt{c}$ 记惟一的元素 $d \in 1 + 4\mathbb{Z}_q$, 使得 $d^2 = c$. 给定两个数 $a, b \in \mathbb{Z}_q$, 使得 $a/b \in 1 + 8\mathbb{Z}_q$, 则 $a' = (a+b)/2$ 和 $b' = b\sqrt{a/b}$ 也属于 $\mathbb{Z}_q$ 且 $a'/b' \in 1 + 8\mathbb{Z}_q$. 更进一步, 若 $a, b \in 1 + 4\mathbb{Z}_q$, 则 $a', b' \in 1 + 4\mathbb{Z}_q$. 然而由 (11.1) 式可以看出, AGM 序列当且仅当 $a/b \in 1 + 16\mathbb{Z}_q$ 时才能收敛. 对于 $a/b \in 1 + 8\mathbb{Z}_q$, AGM 序列可能不收敛.

设 $a, b \in 1 + 4\mathbb{Z}_q$, $a/b \in 1 + 8\mathbb{Z}_q$, $E_{a,b}$ 记下列椭圆曲线

$$E_{a,b}: \quad y^2 = x(x - a^2)(x - b^2).$$

注意, $E_{a,b}$ 并不是一个极小 Weierstrass 模型, 因它模 2 的约化是奇异的. 下面的引理给出了 $E_{a,b}$ 到一个极小 Weierstrass 模型的同构：

引理 11.1　设 $a, b \in 1 + 4\mathbb{Z}_q$, $a/b \in 1 + 8\mathbb{Z}_q$, $E_{a,b}$ 如上, 则同构

$$(x, y) \longmapsto \left(\frac{x - ab}{4}, \frac{y - x + ab}{8}\right)$$

将 $E_{a,b}$ 变为

$$y^2+xy=x^3+rx^2+sx+t,$$

其中

$$\begin{aligned} r&=\frac{-a^2+3ab-b^2-1}{4},\\ s&=\frac{-a^3b+2a^2b^2-ab^3}{8},\\ t&=\frac{-a^4b^2+2a^3b^3-a^2b^4}{64}, \end{aligned} \tag{11.2}$$

且有 $r\in 2\mathbb{Z}_q$, $s\in 8\mathbb{Z}_q$, $t\equiv -(\frac{a-b}{8})^2 \pmod{16}$, 它们定义了一个极小 Weierstrass 模型.

证明 在 $E_{a,b}$ 的方程中代入逆映射

$$(x,y)\longmapsto (4x+ab, 8y+4x),$$

并且除以 64, 就得出 r,s,t 的值. 因为 $a\equiv b \pmod 8$ 且 $a\equiv b\equiv 1 \pmod 4$, 故可令 $a=1+4u+8\alpha$, $b=1+4u+8\beta$, $u,\alpha,\beta\in\mathbb{Z}_q$. 将此代入 (11.2) 式中表明 $r\in 2\mathbb{Z}_q$, $s\in 8\mathbb{Z}_q$, 且

$$t\equiv -(\alpha-\beta)^2\equiv -\Big(\frac{a-b}{8}\Big)^2 \pmod{16}.$$

为了证明这是一个极小 Weisrstras 模型, 只要证明 $\mathrm{ord}_2(c_4)<4$, 因为 $c_4=(1+4r)^2-48s$. 我们易知确实如此, 证毕.

下述引理表明 AGM 迭代构造了一系列椭圆曲线, 它们是 2 同种的, 这就给出了 AGM 迭代和典范提升之间的联系:

引理 11.2 设 $a,b\in 1+4\mathbb{Z}_q$, $a/b\in 1+8\mathbb{Z}_q$, $E_{a,b}$ 定义如前, 令 $a'=(a+b)/2$, $b'=\sqrt{ab}$, 再令

$$E_{a',b'}:\quad y^2=x(x-a'^2)(x-b'^2),$$

则 $E_{a,b}$ 和 $E_{a',b'}$ 是 2 同种的, 且该同种由下式给出:

$$\begin{aligned} \phi:\quad & E_{a,b} && \longrightarrow && E_{a',b'}\\ & (x,y) && \longmapsto && \Big(\frac{(x+ab)^2}{4x}, y\frac{(x-ab)(x+ab)}{8x^2}\Big), \end{aligned} \tag{11.3}$$

且 ϕ 的核是 $\langle(0,0)\rangle$. 更进一步, ϕ 在不变微分上的作用是

$$\phi^*\Big(\frac{dx}{y}\Big)=2\frac{dx}{y}. \tag{11.4}$$

证明 可以完全类似例 3.1 进行证明.

设 $\overline{E}$ 是 $\mathbb{F}_q$ 上一条通常的椭圆曲线, 其方程为

$$\overline{E}:\quad y^2+xy=x^3+c,\qquad c\in\mathbb{F}_q^*.$$

设 E 是 $\overline{E}$ 的典范提升. 任取 $r\in\mathbb{Z}_q$, 使得 $r^2\equiv c \pmod 2$, 置 $a_0=1+4r$, $b_0=1-4r$, 则引理 11.1 表明 E_{a_0,b_0} 同构到 $\overline{E}$ 到 $\mathbb{Z}_q$ 的一个提升, 因此 $j(E_{a_0,b_0})\equiv j(\overline{E}) \pmod 2$.

设 $(a_k,b_k)_{k=0}^{\infty}$ 是相应的 AGM 序列, 考虑椭圆曲线 E_{a_k,b_k}, 引理 11.2 意味着

$$\Phi_2\big(j(E_{a_k,b_k}),j(E_{a_{k+1},b_{k+1}})\big)=0.$$

直接计算表明 $j(E_{a_{k+1},b_{k+1}})\equiv j(E_{a_k,b_k})^2 \pmod 2$. 我们需要下面的

引理 11.3 设 $\mathbb{Q}_q$ 是 $\mathbb{Q}_p$ 的一个非分歧扩张, $\mathbb{Z}_q$ 是 $\mathbb{Q}_q$ 的赋值环. $g\in\mathbb{Z}_q[X,Y]$, 设 $x_0,y_0\in\mathbb{Z}_q$, 满足

$$g(x_0,y_0)\equiv 0 \pmod p,\quad \frac{\partial g}{\partial X}(x_0,y_0)\equiv 0 \pmod p,\quad \frac{\partial g}{\partial Y}(x_0,y_0)\not\equiv 0 \pmod p,$$

则下列性质成立:

1. 对每一个 $x\in\mathbb{Z}_q$ ($x\equiv x_0 \pmod p$), 存在惟一的 $y\in\mathbb{Z}_q$, 使得 $y\equiv y_0 \pmod p$ 且 $g(x,y)=0$;

2. 设 $x'\in\mathbb{Z}_q$, $x\equiv x' \pmod{p^M}$, $M\geqslant 1$, 设 $y'\in\mathbb{Z}_q$ 是满足 $y'\equiv y_0 \pmod p$ 且 $g(x',y')=0$ 的惟一的元素, 则 $y'\equiv y \pmod{p^{M+1}}$.

证明 定义 $h\in\mathbb{Z}_q[Y]$ 如下: $h(Y)=g(x,Y)$, 则 $h(y_0)\equiv 0 \pmod p$ 且 $h'(y_0)\equiv \frac{\partial g}{\partial Y}(x_0,y_0)\not\equiv 0 \pmod p$. 于是 Hensel 引理给出了惟一的 $y\in\mathbb{Z}_q$, 使得 $h(y)=g(x,y)=0$ 且 $y\equiv y_0 \pmod p$. 这就证明了引理的第 1 部分. 更进一步, 给定 x, 我们可以对 $g(x,y)$ 和 $y_0 \bmod p$ 应用牛顿迭代计算 y 到任意精度. 为证明第二部分, 令

$$\delta_x=x'-x,\qquad \delta_y=y'-y.$$

显然 $\delta_x\equiv\delta_y\equiv 0 \pmod{p^M}$. 写出 $g(X,Y)$ 的泰勒展开式有

$$\begin{aligned}0=g(x',y')&=g(x+\delta_x,y+\delta_y)=\sum_{i,j}g_{i,j}(x+\delta_x)^i(y+\delta_y)^j\\&=\sum_{i,j}g_{i,j}(x^i+ix^{i-1}\delta_x+\delta_xR_x(x))(y^j+jy^{j-1}\delta_y+\delta_y^2R_y(y)),\end{aligned}\tag{11.5}$$

其中 R_x 和 R_y 是系数在 $\mathbb{Z}_q$ 中的多项式. 因 $\delta_x^2\equiv\delta_y^2\equiv 0 \pmod{p^{2M}}$ 且 $M\geqslant 1$, 故有

$$0\equiv\frac{\partial g}{\partial X}(x,y)(x-x')+\frac{\partial g}{\partial y}(x,y)(y-y') \pmod{p^{M+1}}.$$

上述方程意味着 $y \equiv y' \pmod{p^{M+1}}$(因为 $\delta_x \equiv 0 \pmod{p^M}$, $\frac{\partial g}{\partial X}(x,y) \equiv 0 \pmod{p}$, 且 $\frac{\partial g}{\partial Y}(x,y) \not\equiv 0 \pmod{p}$), 证毕.

现将引理 11.3 应用到模多项式 $\Phi_2(X,Y)$ 和点 $\big(j(E_{a_{k+1},b_{k+1}}), j(E_{a_k,b_k})\big)$, 并注意到 $j(E_{a_0,b_0}) \equiv j(\overline{E}) \pmod{2}$, 故结合 Lubin-Serre-Tate 关于椭圆曲线典范提升的结果得出

$$j(E_{a_k,b_k}) \equiv \Sigma^k\big(j(E)\big) \pmod{2^{k+1}}, \tag{11.6}$$

其中 Σ 是 Frobenius 在 $\mathbb{Z}_q$ 上的提升, 而 Σ^k 表示 k 个 Σ 的复合映射.

注记 11.1 尽管 AGM 序列 $(a_k,b_k)_{k=0}^{\infty}$ 本身并不一定收敛, 但椭圆曲线序列 $(E_{a_k,b_k})_{k=0}^{\infty}$ 在下述意义下收敛: $\lim_{k\to\infty} j(E_{a_k,b_k})$ 存在且等于 $\overline{E}$ 的典型提升的 j 不变量.

由上面的讨论, 我们知道 AGM 序列本质上给出了计算 $\overline{E}$ 的典范提升 E 的 j 不变量的一个有效算法. 事实上, 我们可以得到更多的信息. 下面就来讨论这一点.

§11.2 计算 Frobenius 映射的迹

设 $a, b \in 1+4\mathbb{Z}_q$, $a/b \in 1+8\mathbb{Z}_q$, 使得 $j(E_{a,b}) = j(E)$. 设 $(a',b') = (\frac{a+b}{2}, \sqrt{ab})$, ϕ: $E_{a,b} \to E_{a',b'}$ 是 §11.1 中的 AGM 序列定义的 2 同种映射. 而 Σ: $E_{a,b} \to E_{\Sigma(a),\Sigma(b)}$ 是 2 次幂 Frobenius 映射的提升. 于是我们有下面的图 11.1:

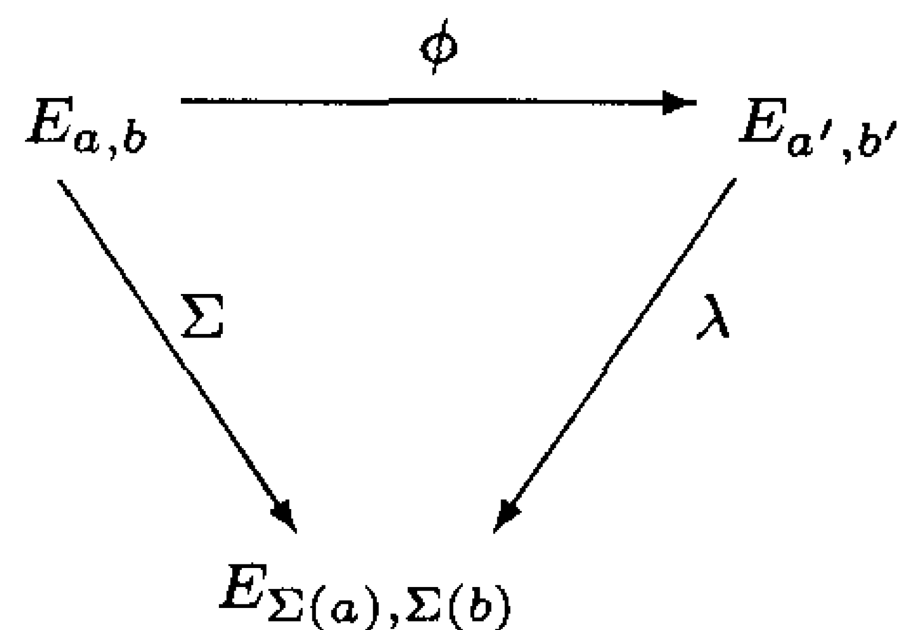


图 11.1

Frobenius 同种 Σ: $E_{a,b} \to E_{\Sigma(a),\Sigma(b)}$ 的核是下述 2-torsion 群:

$$E_{a,b}[2] = \{\mathcal{O}, (0,0), (a^2,0), (b^2,0)\}$$

的一个 2 阶子群.

应用引理 11.1 中给出的同构, 分析在一个极小模型上的 2-torsion 点的约化. 直接计算表明 $(0,0)$ 映射到 $\mathcal{O}$, 而 $(a^2,0)$ 和 $(b^2,0)$ 映射到 $(0, \frac{a-b}{8} \pmod{2})$, 故知道 $\ker\Sigma = \{\mathcal{O}, (0,0)\}$. 引理 11.2 表明 $\ker\Sigma = \ker\phi$. 因为 ϕ 和 Σ 都是可分的, 存在一个同构 λ: $E_{a',b'} \to E_{\Sigma(a),\Sigma(b)}$, 使得 $\Sigma = \lambda \circ \phi$.

引理 11.4 给定 $\mathbb{Q}_q$ 上 2 条椭圆曲线 $E_{a,b}: y^2 = x(x-a^2)(x-b^2)$ 和 $E_{c,d}: y'^2 = x'(x'-c^2)(x'-d^2)$, 其中 $a,b,c,d \in 1+4\mathbb{Z}_q$, $a/b, c/d \in 1+8\mathbb{Z}_q$, 则 $E_{a,b}$ 和 $E_{c,d}$ 是同构的当且仅当 $x' = u^2x$, $y' = u^3y$, 其中 $u^2 = \frac{c^2+d^2}{a^2+b^2}$. 且有 $(a/b)^2 = (c/d)^2$ 或 $(a/b)^2 = (d/c)^2$.

证明 设 λ: $E_{a,b} \to E_{c,d}$ 是一个同构, 则 λ 的一般形式为

$$(x,y) \mapsto (u^2x + r, u^3y + u^2sx + t), \quad u \in \mathbb{Q}_q^*, r,s,t \in \mathbb{Q}_q,$$

其中 u,r,s,t 满足 §3.1 中的关系式 (3.12).

由 §3.1 中的关系式 (3.12) 中第 1 方程和第 3 方程可知 $s = t = 0$, 剩下的方程则给出

$$u^2(a^2+b^2) = c^2 + d^2 - 3r, \tag{11.7}$$

$$0 = r(r-c^2)(r-d^2). \tag{11.8}$$

(11.8) 式表明 $r = 0$, $r = c^2$ 或 $r = d^2$. 设 $r \neq 0$, 则由 (11.7) 式导出矛盾：因为 $\operatorname{ord}_2\big(u^2(a^2+b^2)\big)$ 为奇数, 而 $\operatorname{ord}_2(c^2+d^2-3r)$ 将为零, 故 $r = 0$, 从而 $u^2 = \frac{c^2+d^2}{a^2+b^2}$. 在 $E_{c,d}$ 的方程中代入 $x' = u^2x$ 和 $y' = u^3y$, 并除以 u^6, 有

$$(x-a^2)(x-b^2) = \left(x - \frac{c^2}{u^2}\right)\left(x - \frac{d^2}{u^2}\right).$$

由于上式左右两端均分解为 2 个 1 次因子之积, 故必有

$$a^2 = c^2/u^2 \quad 且 \quad b^2 = d^2/u^2,$$

或

$$a^2 = d^2/u^2 \quad 且 \quad b^2 = c^2/u^2,$$

即

$$(a/b)^2 = (c/d)^2 \quad 或 \quad (a/b)^2 = (d/c)^2.$$

证毕.

现在记 ω 和 ω' 分别是 $E_{a,b}$ 和 $E_{\Sigma(a),\Sigma(b)}$ 的不变微分, 则

$$\Sigma^*(\omega') = (\lambda \circ \phi)^*(\omega') = 2u^{-1}\omega,$$

其中 $u^2 = \frac{\Sigma(a)^2+\Sigma(b)^2}{a'^2+b'^2}$. 定义 $\xi = a/b = 1+8c$, $\xi' = a'/b' = 1+8c'$, 则引理 11.4 意味着

$$\xi'^2 = \Sigma(\xi)^2 \quad 或 \quad \xi'^2 = \frac{1}{\Sigma(\xi)^2}.$$

在上面的方程中代入 $\xi = 1 + 8c$ 和 $\xi' = 1 + 8c'$ 并除以 16, 得出 $c' \equiv \Sigma(c) \pmod 4$ 或 $c' \equiv -\Sigma(c) \pmod 4$. 而 $1 + 8c' = (1 + 4c)/\sqrt{1 + 8c} \pmod{32}$ 的泰勒展开式表明 $c' \equiv c^2 \pmod 4$, 因为在第一次迭代后, c 本身是一个平方 $\alpha^2 \pmod 4$, 且 $\Sigma(\alpha^2) \equiv \alpha^4 \pmod 4$, 故有 $\xi'^2 = \Sigma(\xi)^2$. 在 u^2 的表达式中代入 $b'^2 = a'^2\Sigma(b)^2/\Sigma(a)^2$, 并开平方根, 得到

$$u = \pm\Sigma(a)/a'. \tag{11.9}$$

现设 $(a_k, b_k)_{k=0}^{\infty}$ 是 $(a_0 = a, b_0 = b)$ 的 AGM 序列, 考虑下述图表:

$$\begin{array}{ccccccccc} E_{a,b} & \xrightarrow{\phi_0} & E_{a_1,b_1} & \xrightarrow{\phi_1} & E_{a_2,b_2} & \xrightarrow{\phi_2} & \cdots & \xrightarrow{\phi_{n-1}} & E_{a_n,b_n} \\ \text{id.}\downarrow & & \lambda_1\downarrow & & \lambda_2\downarrow & & \downarrow & & \lambda_n\downarrow \\ E_0 & \xrightarrow{\Sigma_0} & E_1 & \xrightarrow{\Sigma_1} & E_2 & \xrightarrow{\Sigma_2} & \cdots & \xrightarrow{\Sigma_{n-1}} & E_n = E_0 \end{array} \tag{11.10}$$

其中 $E_k = E_{\Sigma^k(a),\Sigma^k(b)}$, $\Sigma_k : E_k \to E_{k+1}$ 是 2 次 Frobenius 同种的提升.

因为 $\ker(\Sigma_k \circ \lambda_k) = \ker(\phi_k)$, $\forall k \in \mathbb{N}$, 我们可以重复图表图 11.1 中的推理, 找出一个同构 λ_{k+1}, 使得 $\Sigma_k = \lambda_{k+1} \circ \phi_k \circ \lambda_k^{-1}$. 因为假定 $E_{a,b}$ 同构到 $\overline{E}$ 的典范提升, 则

$$\mathrm{Tr}\big(\Sigma_{n-1} \circ \cdots \Sigma_0\big) = \mathrm{Tr}\mathcal{F} = \mathrm{Tr}\overline{F},$$

其中 $\overline{F}$ 是 $\overline{E}$ 的 Frobenius 同种, 而 $\mathcal{F}$ 是 $\overline{F}$ 在 Lubin-Serre-Tate 典范同构下的像.

上面的图表 (11.10) 表明 $\Sigma_{n-1} \circ \cdots \circ \Sigma_0 = \lambda_n \circ \phi_{n-1} \circ \cdots \circ \phi_0$, 由于 ϕ_k 作用在不变微分上相当于乘 2, 而 λ_n 作用在不变微分上相当于乘 $\pm a_n/a_0$, 故有

$$\mathcal{F}^*(\omega) = \pm 2^n \frac{a_n}{a_0}(\omega).$$

Weil 猜想意味着 Frobenius 的特征多项式的根之积等于 2^n, 故

$$\mathrm{Tr}\mathcal{F} = \mathrm{Tr}\overline{F} = \pm\frac{a_0}{a_n} \pm 2^n \frac{a_n}{a_0}. \tag{11.11}$$

注记 11.2 若曲线 $\overline{E}$ 由方程 $y^2 + xy = x^3 + a (a \in \mathbb{F}_q^*)$ 定义, 则 $(\sqrt[4]{a}, \sqrt[2]{a})$ 是一个 4 阶点, 从而 $\mathrm{Tr}\overline{F} \equiv 1 \pmod 4$. 因为 $a_0/a_n \in 1 + 4\mathbb{Z}_q$, 故可以在 (11.11) 式中选择正确的符号, 得到 $\mathrm{Tr}(\overline{F}) \equiv a_0/a_n \pmod q$.

在前面的讨论中, 我们假定了 $a, b \in 1 + 4\mathbb{Z}_q$, $a/b \in 1 + 8\mathbb{Z}_q$, 使得 $j(E_{a,b}) = j(E)$. 但实际的情形是: 只有 a 和 b 的近似值, 而并没有它们的精确值.

现设 $\overline{E}$ 是由

$$\overline{E}: \ y^2 + xy = x^3 + c, \quad c \in \mathbb{F}_q^*$$

定义的一条通常 (ordinary) 椭圆曲线. 任取 $r \in \mathbb{Z}_q$, 使得 $r^2 \equiv c \pmod 2$, 并令 $a_0 = 1 + 4r$, $b_0 = 1 - 4r$. 由第一节中的 (11.5) 式知道, 如果 $(a_k, b_k)_{k=0}^{\infty}$ 是 AGM 序

列, 则

$$j(E_{a_k,b_k}) \equiv j(E_k) \pmod{2^{k+1}},$$

其中 $E_k = \Sigma^k(E)$ 是 $\sigma^k(\overline{E})$ 的典范提升. 将 $j(E_{a_k,b_k})$ 表作 a_k, b_k 的函数表明, a_k 和 b_k 必须精确到模 2^{k+3}, 因此有

$$\mathrm{Tr}\overline{F} \equiv \frac{a_{N-3}}{a_{N-3+n}} + 2^n \frac{a_{N-3+n}}{a_{N-3}} \pmod{2^N},$$

其中 $N = \lceil \frac{n}{2} \rceil + 2$, 由上式即可惟一定出 $\mathrm{Tr}\overline{F}$ 来. 于是我们可以总结 AGM 算法如下:

(算法 11.1) AGM 算法 (I)

输入: 椭圆曲线 $\overline{E}$: $y^2 + xy = x^3 + c$, $c \in \mathbb{F}_{2^n}^*$, $j(\overline{E}) \notin \mathbb{F}_4$.

输出: $\overline{E}$ 在 $\mathbb{F}_{2^n}$ 上的有理点之数目.

Step 1: 令 $N = \lceil \frac{n}{2} \rceil + 2$;

Step 2: 任取 $r \in \mathbb{Z}_q$ 使 $r \equiv \sqrt{c} \pmod 2$;

Step 3: 令 $a = 1 + 4r$, $b = 1 - 4r$;

Step 4: 对 $i = 4$ 到 N, 计算下列循环:

$$(a, b) \equiv \Big(\frac{a+b}{2}, \sqrt{ab}\Big) \pmod{2^i}$$

Step 5: 令 $a_0 = a$;

Step 6: 对 $j = 0$ 到 $n - 1$, 计算下列循环:

$$(a, b) \equiv \Big(\frac{a+b}{2}, \sqrt{ab}\Big) \pmod{2^N}$$

Step 7: $t \equiv a_0/a \pmod{2^N}$;

Step 8: 若 $t^2 > 2^{n+2}$, 则令 $t = t - 2^N$;

Step 9: 输出 $2^n + 1 - t$.

显然, 上述算法的复杂度由 Step 4 和 Step 6 决定, 它们要求 $O(n)$ 个平方根运算, 精度要求到 $O(n)$. 因为每一个平方根计算要求 $O(1)$ 个乘法, 故上述算法的复杂度为 $O(n^{2\mu+1})$, 而存储空间显然是 $O(n^2)$, 因为只有 $\mathbb{Z}_q/2^N\mathbb{Z}_q$ 中 $O(1)$ 个元素需要存储.

注记 11.3 上述算法中的 Step 6 也可以由 1 次 AGM 迭代和 1 个范 (Norm) 计算来替代. 实际上, 方程 (11.9) 表明

$$\Sigma_0^*\Big(\frac{dx}{y}\Big) = \pm\frac{a_1}{\Sigma(a_0)}\Big(\frac{dx}{y}\Big),$$

因为所有曲线 E_k 是共轭的, 故有

$$\mathcal{F}^*\left(\frac{dx}{y}\right) = \pm 2^n N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{a_1}{\Sigma(a_0)}\right)\left(\frac{dx}{y}\right) = \pm 2^n N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{a_1}{a_0}\right)\left(\frac{dx}{y}\right).$$

因此, 只要用 1 次 AGM 迭代算出 a_1(在 Step 6 中), 然后置 $t \equiv N_{\mathbb{Q}_q/\mathbb{Q}_p}(a_0/a_1)$ $(\bmod\ 2^N)$ (在 Step 7 中). 于是我们有:

(算法 11.2) AGM 算法 (II)

输入: 椭圆曲线 $\overline{E}$: $y^2 + xy = x^3 + c$, $c \in \mathbb{F}_{2^n}^*$, $j(\overline{E}) \notin \mathbb{F}_4$.
输出: $\overline{E}$ 在 $\mathbb{F}_{2^n}$ 上的有理点之数目.
Step 1: 令 $N = \lceil \frac{n}{2} \rceil + 2$;
Step 2: 任取 $r \in \mathbb{Z}_q$, 使得 $r \equiv \sqrt{c}\ (\bmod\ 2)$;
Step 3: 令 $a = 1 + 4r$, $b = 1 - 4r$;
Step 4: 对 $i = 4$ 到 N, 计算下列循环:

$$(a, b) \equiv \left(\frac{a+b}{2}, \sqrt{ab}\right) \quad (\bmod\ 2^i)$$

Step 5: 令 $a_0 = a$, $b_0 = b$;
Step 6: 令 $a_1 = \frac{a_0 + b_0}{2}$;
Step 7: $t \equiv N_{\mathbb{Q}_q/\mathbb{Q}_p}(a_0/a_1)\ (\bmod\ 2^N)$;
Step 8: 若 $t^2 > 2^{n+2}$, 则令 $t = t - 2^N$;
Step 9: 输出 $2^n + 1 - t$.

但是如果使用 AGM 算法 (II), 则一种有效的快速范 (Norm) 数计算算法就是必要的了. 下面就来讨论这个问题.

§11.3 范数的快速算法

设 $\mathbb{Q}_p$ 是 p-adic 数域, 记 $K = \mathbb{Q}_q$, $q = p^N$, 是 $\mathbb{Q}_p$ 的 N 次非分歧扩张. 下面将给出计算 $N_{K/\mathbb{Q}_p}(x)$ 的一个快速算法, 其中 $x \in 1 + 4\mathbb{Z}_q$(若 $p = 2$) 或 $x \in \mathbb{Z}_q^*$(若 $p \geqslant 3$). 记 $|\cdot|_p$ 是正规化的 p-adic 赋值, $|p|_p = p^{-1}$. 记

$$\nu_p := \begin{cases} 2, & 若\ p = 2, \\ 1, & 若\ p \neq 2. \end{cases}$$

令 $U := p^{\nu_p} R$, 其中 $R = \mathbb{Z}_q$ 是 K 的赋值环. U 是下面将要定义的指数函数的收敛区域.

首先, 设 $x \in 1+U$, 则 $\sigma \in \mathrm{Gal}(K/\mathbb{Q}_p)$ 保持 p-adic 赋值, 从而 σ 是一个连续映射, 有 $\sigma(\log x) = \log \sigma(x)$, 其中

$$\log x := \sum_{i=1}^{\infty} \frac{(-1)^{i-1}(x-1)^i}{i}.$$

注意到 $N_{K/\mathbb{Q}_p}(x) = \prod_{j=1}^{n} \sigma^j(x)$, $\mathrm{tr}_{K/\mathbb{Q}_p}(x) = \sum_{i=1}^{n} \sigma^j(x)$, 有

$$\log N_{K/\mathbb{Q}_p}(x) = \mathrm{Tr}_{K/\mathbb{Q}_p}(\log x), \quad \forall |x-1|_p < 1.$$

因为

$$\exp(x) := \sum_{i=0}^{\infty} \frac{x^i}{i!}, \quad x \in U$$

收敛, 故有

$$N_{K/\mathbb{Q}_p}(x) = \exp\left(\mathrm{Tr}_{K/\mathbb{Q}_p}(\log x)\right), \quad \forall x \in U.$$

注意, 对于 $x \in U$, 为了计算 $N_{K/\mathbb{Q}_p}(x) \pmod{p^M}$, 需要计算 $\mathrm{Tr}_{K/\mathbb{Q}_p}(\log x) \pmod{p^M}$, 于是问题归纳到如何快速计算上面的幂级数和 $\mathrm{Tr}_{K/\mathbb{Q}_p}$.

设 $H(X)=\sum_{i=0}^{N} h_i X^i \in \mathbb{Z}_p[X]$ 是一个 N 次首一不可约多项式, 使得 $H(X) \bmod p$ 是 $\mathbb{F}_p[X]$ 中不可约的, 令 ρ 记 X 在 $\mathbb{Q}_p[X]/(H(X))$ 中的类, 于是 $R = \mathbb{Z}_p[\rho]$, $K = \mathbb{Q}_p[\rho]$. 现在设 t 为正整数, 给定 $x \bmod p^M$, 则 $x^{p^t} \bmod p^{M+t}$ 是有意义的且 $\mathrm{ord}_p(x^{p^t} - 1) \geqslant t + \mathrm{ord}_p(x-1)$. 令 l_p 是计算 p 次幂所需乘法的次数, 则可以用 $R/p^{M+t}R$ 上 $2\sqrt{l_p M} + O(\log M)$ 个乘法算出

$$\sum_{i<(t+\nu_p)-[\log_p i]<M} \frac{(-1)^{i-1}}{i}\left(x^{p^t}-1\right)^i \pmod{p^{M+t}}, \tag{11.12}$$

其中 $t = [\sqrt{M/l_p}]$. 于是可得出 $\log x \bmod p^M = p^{-t}\left(\log x^{p^t} \bmod p^{M+t}\right)$. 对于 $p=2$, 还可以有更好的结果：令 $t = [\sqrt{M/2}]$, 置 $\gamma = \frac{z}{2+z}$, $z = x^{2^t} - 1$, 于是 $x^{2^t} = \frac{1+\gamma}{1-\gamma}$. 对于一个给定的 $x \bmod 2^M$, $x \in 1+U$, 易知 $\gamma \bmod 2^{M+t-1}$ 是有意义的且 $\mathrm{ord}_2 \gamma \geqslant t + \nu_p - 1 \geqslant t+1$, 从而

$$\log x^{2^t} \equiv \left(2 \sum_{1 \leqslant (t+1)(2i-1) < M+t} \frac{\gamma^{2i-1}}{2i-1}\right) \pmod{2^{M+t}}, \tag{11.13}$$

它可以用 $R/2^{M+t}R$ 上 $\sqrt{2M} + O(1)$ 个乘法算出.

现在, 假定已经获得了 $a_i \in \mathbb{Z}$, 使得 $\log x \equiv \sum_{i=0}^{N-1} a_i \rho^i \pmod{p^M}$, 则

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(\log x) \equiv \sum_{i=0}^{N-1} a_i \mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^i) \pmod{p^M},$$

而其中每一个 $\mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^i)$, $1 \leqslant i < N$, 可以用牛顿关系式

$$\mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^i) + \sum_{j=1}^{i-1} \mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^{i-j}) h_{N-j} + i h_{N-i} = 0$$

归纳地算出. 这可以在预运算中进行. 因为我们只计算 $\mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^i) \pmod{p^M}$, 故存储这些预运算的值所需空间复杂度为 $O(NM)$.

因为 $x \in 1+U$, 故有 $\mathrm{Tr}_{K/\mathbb{Q}_p}(\log x) \in U \cap \mathbb{Q}_p$. 选取一个整数 $u(0 \leqslant u < p^{M-\nu_p})$, 使得 $p^{\nu_p} u \equiv \mathrm{Tr}_{K/\mathbb{Q}_p}(\log x)$, 则 $N_{K/\mathbb{Q}_p}(x) \equiv B^u \pmod{p^M}$, 其中

$$B = \sum_{i=0}^{[M/(\nu_p-(p-1)^{-1})]} \frac{(p^{\nu_p})^i}{i!} \equiv \exp(p^{\nu_p}) \pmod{p^M}$$

(注意 $\mathrm{ord}_p(i!) = \sum_{j=1}^{\infty} [i/p^j] \leqslant \frac{i}{p-1}$). 在计算幂次 B^u 时, 注意利用通常的基于 u 的二进制表示. 于是下面的算法就可以计算出 $N_{K/\mathbb{Q}_p}(x)$, $\forall x \in 1+U$, 其中的时间和空间复杂度分别为 $O(\max(\sqrt{M} T_{M+t,N}, MT_M, NT_M))$ 和 $O(MN)$. 其中 T_M 表示完成 $\mathbb{Z}/p^M\mathbb{Z}$ 上一个算术所需比特运算次数, 而 $T_{a,b}$ 表示完成 $\wp_{a,b}$ 上一个算术运算所需要比特运算次数, 其中 $\wp_{a,b} = \{f(x) \in \mathbb{Z}[x]/p^a\mathbb{Z}[x] |\ \deg(f) < b\}$.

在下面的算法中, 我们记: $B = \exp(p^{\nu_p}) \pmod{p^M}$, $\beta_i = \mathrm{Tr}_{K/\mathbb{Q}_p}(\rho^i) \pmod{p^M} \in \mathbb{Z}/p^M\mathbb{Z}$, $0 \leqslant i \leqslant N-1$. 它们都是经预运算计算出来的.

(算法 11.3) 快速范数 (Norm) 算法

输入: $x \bmod p^M R$, $x \in 1+U$, B, β_i, $0 \leqslant i \leqslant N-1$.

输出: $N_{K/\mathbb{Q}_p}(x) \bmod p^M$.

Step 1: 令 $t = [\sqrt{M/l_p}]$(若 $p \neq 2$) 或 $t = [\sqrt{M/2}]$(若 $p = 2$);

Step 2: 计算 $z \equiv x^{p^t} - 1 \pmod{p^{M+t}}$; (注意这是有意义的);

Step 3: 计算 $w \equiv \log(1+z) \pmod{p^{M+t}}$; (若 $p \neq 2$, 用 (11.12) 计算, 若 $p = 2$, 用 (11.13) 计算);

Step 4: 计算 $w \equiv p^{-t} w \pmod{p^M}$; $(= \log x \pmod{p^M})$;

Step 5: 计算 $a_i \in \mathbb{Z}/p^M\mathbb{Z}$, 使得 $w = \sum_{i=0}^{N-1} a_i \rho^i$;

Step 6: 计算出整数 u, 使得 $0 \leqslant u < p^{M-\nu_p}$ 且 $p^{\nu_p} u \equiv \sum_{i=0}^{N-1} a_i \beta_i \pmod{p^M}$;

Step 7: 输出 B^u.

因为我们特别关注 $p = 2$ 时的情形, 所以将上述算法在 $p = 2$ 时的情形单独写出来.

(算法 11.4) 特征 2 的范数算法

输入：一个元素 $a \in 1 + 4\mathbb{Z}_q$, 精度 M.

输出：$N_{K/\mathbb{Q}_p}(a) \bmod 2^M$.

Step 1: 令 $s = \lfloor \sqrt{M}/2 \rfloor$;

Step 2: $z \equiv a^{2^s} - 1 \pmod{2^{M+s}}$;

Step 3: $w \equiv \log(1+z) \pmod{2^{M+s}}$(用 (11.13) 式计算);

Step 4: $w \equiv 2^{-s} w \pmod{2^M}$;

Step 5: 计算 $a_i \in \mathbb{Z}/2^M\mathbb{Z}$, 使得 $w = \sum_{i=0}^{N-1} a_i \rho^i$;

Step 6: $u = 4^{-1} \sum_{i=0}^{N-1} a_i \beta_i$;

Step 7: 输出 $\exp(4)^u \bmod 2^M$.

其中的 β_i 和 $\exp(4)$ 由预运算给出. 在第 7 步中, 将 u 表为二进制, 然后利用通常的幂次计算方法.

下面我们介绍范数计算的另一种方法, 它是基于范数与结式关系的一种算法.

设 $\mathbb{Z}_q = \mathbb{Z}_p[\theta]$, θ 是 n 次首一不可约多项式 $f(x) \in \mathbb{Z}_p[x]$ 的一个根, 于是 $f(x)$ 在 $\mathbb{Z}_q$ 上完全分裂为 $f(x) = \prod_{i=0}^{n-1}\left(x - \Sigma^i(\theta)\right)$, Σ 是 Frobenius. 对于 $\alpha \in \mathbb{Q}_q$, 有

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(\alpha) = p^{n\mathrm{ord}_p(\alpha)} N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\alpha/p^{\mathrm{ord}_p(\alpha)}\right), \tag{11.14}$$

故只要能计算出 $\mathbb{Z}_q$ 中任意单位的范数, 就可以计算出任意元素的范数.

设 $\alpha = \sum_{i=0}^{n-1} a_i\theta^i$ 是 $\mathbb{Z}_q$ 中单位, 定义 $A(x) = \sum_{i=0}^{n-1} a_i x^i \in \mathbb{Z}_p[x]$, 由范数和结式的定义, 有

$$N_{\mathbb{Q}_q/\mathbb{Q}_p}(\alpha) = \prod_{i=0}^{n-1} \Sigma^i(\alpha) = \prod_{i=0}^{n-1} A\left(\Sigma^i(\theta)\right) = \mathrm{Res}\left(f(x), A(x)\right), \tag{11.15}$$

结式 $\mathrm{Res}\left(f(x), A(x)\right)$ 可按下述方法计算, 此方法称为 Moenck 算法.

设 $f = f_n x^n + \cdots + f_0 \in \mathbb{K}[x]$ 是域 $\mathbb{K}$ 上一个 n 次多项式, 定义

$$f|k = f_n x^k + \cdots + f_{n-k}, \tag{11.16}$$

此处 $f_i = 0\ (\forall i < 0)$, 称 2 个多项式对 (f, g) 和 (f^*, g^*) 是重合到·k 的, 如果

$$f|k = f^*|k, \qquad g|\left(k - (\deg f - \deg g)\right) = g^*|\left(k - (\deg f^* - \deg g^*)\right). \tag{11.17}$$

给定 2 个首一多项式 r_0 和 r_1, $\deg r_0 > \deg r_1$, 则用带余除法计算出表达式

$$r_{i-1} = q_i r_i + p_{i+1} r_{i+1}, \tag{11.18}$$

其中 $q_i, r_i \in \mathbb{K}[x]$, $p_{i+1} \in \mathbb{K}$, $0 \leqslant i \leqslant l$, 每个 r_i 是首一的, 且 $r_{l-1} = q_l r_l$. 令 $m_i = \deg q_i$, 对于 $k \in \mathbb{N}$, 定义

$$\eta(k) = \max\left\{0 \leqslant j \leqslant l \,\middle|\, \sum_{1\leqslant i\leqslant j} m_i \leqslant k\right\}. \tag{11.19}$$

Moenck 算法的基础是下述引理, 它表明, 在欧氏除法中的商仅仅取决于输入多项式的最高次系数.

引理 11.5 设 $k \in \mathbb{N}$, 而 (f,g) 和 (f^*,g^*) 重合到 $2k$, 则对一切 $1 \leqslant i \leqslant \eta(k)$, 有 $\eta(k) = \eta^*(k)$, $q_i = q_i^*$, $p_{i+1} = p_{i+1}^*$, 其中 q_i, q_i^* 分别是欧氏除法 (f,g) 和 (f^*,g^*) 的商, 而 p_{i+1} 和 p_{i+1}^* 分别是欧氏除法 (f,g) 和 (f^*,g^*) 的余式的首项系数.

证明 首先证明下述结论: 设 (f,g), $(f^*,g^*) \in \big(\mathbb{K}[x]/\{0\}\big)^2$ 重合到 $2k$, $k \geqslant \deg f - \deg g \geqslant 0$, 令

$$f = qg + r, \qquad \deg r < \deg g,$$
$$f^* = q^*g^* + r^*, \qquad \deg r^* < \deg g^*,$$

则 $q = q^*$, 且或者 (g,r) 和 (g^*,r^*) 重合到 $2(k-\deg q)$, 或者 $r=0$, 或者 $k - \deg q < \deg g - \deg r$.

为此, 首先将 (f,g) 和 (f^*,g^*) 乘以 x 的适当幂次, 可以假定 $\deg f = \deg f^*$, 则 $\deg g = \deg g^*$, $k \geqslant \deg q = \deg f - \deg g = \deg f^* - \deg g^* = \deg q^*$, 而

$$\begin{aligned}
\deg\big(f - f^*\big) &< \deg f - 2k \leqslant \deg g - k,\\
\deg\big(g - g^*\big) &< \deg g - \big(2k - (\deg f - \deg g)\big) = \deg f - 2k\\
&\leqslant \deg g - k \leqslant \deg g - \deg q,\\
\deg\big(r - r^*\big) &\leqslant \max\{\deg r, \deg r^*\} < \deg g;
\end{aligned} \tag{11.20}$$

并且

$$f - f^* = q(g - q^*) + (q - q^*)g^* + (r - r^*). \tag{11.21}$$

由 (11.20) 式, 多项式 $f - f^*$, $q(g-g^*)$ 和 $r - r^*$ 的次数都比 $\deg g$ 小, 故

$$\deg\big((q-q^*)g^*\big) < \deg g = \deg g^*,$$

这意味着 $q = q^*$. 现在设 $r \neq 0$ 且 $k - \deg q \geqslant \deg g - \deg r$, 必须证明

$$\begin{aligned}
g\big|\big(2(k-\deg q)\big) &= g^*\big|\big(2(k-\deg q)\big),\\
r\big|\big(2(k-\deg q) - (\deg g - \deg r)\big) &= r^*\big|\big(2(k-\deg q) - (\deg g^* - \deg r^*)\big).
\end{aligned} \tag{11.22}$$

第一个式子由 (f,g) 和 (f^*,g^*) 重合到 $2k$ 立得, 另一方面, 有

$$\begin{aligned}\deg(r-r^*)&\leqslant\max\{\deg(f-f^*),\deg q+\deg(g-g^*)\}\\&<\deg q+\deg f-2k=\deg g-2(k-\deg q)\\&=\deg r-\big(2(k-\deg q)-(\deg g-\deg r)\big),\end{aligned}\tag{11.23}$$

由 (11.21) 和 (11.20) 式及上面的假定, 有

$$\deg r\geqslant\deg q+\deg g-k\geqslant\deg q+\deg f-2k,$$

因此 $\deg r=\deg r^*$, 于是 (11.22) 式中第 2 式子由 (11.23) 式中第 2 个等号得出, 这就证明了我们的结论.

现在对 j 用归纳法, 可证得对 $0\leqslant j\leqslant\eta(k)$, 下述事实成立: $j\leqslant\eta^*(k)$, $q_i=q_i^*$ 且 $p_{i+1}=p_{i+1}^*$ (对于 $1\leqslant i\leqslant j$), 或者 $j=\eta(k)$, 或者 (r_j,r_{j+1}) 和 (r_j^*,r_{j+1}^*) 重合到 $2\big(k-\sum_{1\leqslant i\leqslant j}m_i\big)$.

上述事实对于 $j=0$ 显然, 而归纳步骤可由归纳假设和上面证明的结论得出. 而 $j\leqslant\eta^*(k)$ 可由下式得出:

$$\sum_{1\leqslant i\leqslant j}\deg q_i^*=\sum_{1\leqslant i\leqslant j}\deg q_i\leqslant\sum_{1\leqslant i\leqslant h}\deg q_i\leqslant k,$$

因此 $j\leqslant\eta^*(k)$, 引理证毕.

引理 11.6 设 $f,g\in\mathbb{K}[x]$, $\deg f=n_0$, $\deg g=n_1\leqslant n_0$, 令 $n_2,\cdots,n_l$ 是对 (f,g) 做欧氏除法后余式的次数, 而 $\rho_0,\cdots,\rho_l$ 是它们的首项系数, 若 $\gcd(f,g)=1$, 则

$$\mathrm{Res}(f,g)=(-1)^{\tau}\rho_0^{n_1}\prod_{1\leqslant j\leqslant l}\rho_j^{n_{j-1}-n_{j+1}},\tag{11.24}$$

此处 $\tau=\sum_{1\leqslant j\leqslant l}n_{j-1}n_j$, 且该结式可由 $\mathbb{K}$ 中 $O\big(n^{\mu}\log n\big)$ 个运算得出.

证明 首先, 定义任意二个多项式 f 和 g 的 k 阶子结式如下: 设

$$f=\sum_{0\leqslant j\leqslant n}f_jx^j,\quad g=\sum_{0\leqslant j\leqslant m}g_jx^j,\quad f_j,g_j\in\mathbb{K},$$

则定义矩阵 S_k 如下 (若 $j<0$, 则 $f_j=0$, $g_j=0$):

$$S_k(f,g)=\begin{pmatrix} f_n & & \cdots & & g_m & & & & & \\ f_{n-1} & \ddots & \cdots & & g_{m-1} & g_m & & & & \\ \vdots & \ddots & \ddots & & \vdots & & \ddots & & & \\ f_{n-m+k+1} & \cdots & \cdots & f_n & g_{k+1} & g_{k+2} & \cdots & g_m & & \\ \vdots & & & \vdots & \vdots & & & & \ddots & \\ f_{k+1} & \cdots & \cdots & f_m & g_{m-n+k+1} & \cdots & \cdots & \cdots & \cdots & g_m \\ \vdots & & & \vdots & \vdots & & & & & \vdots \\ f_{2k-m+1} & \cdots & \cdots & f_k & g_{2k-n+1} & \cdots & \cdots & \cdots & \cdots & g_k \end{pmatrix},$$

显然 S_k 是一个 $(m+n-2k)$ 阶方阵, 且 S_0 就是对应于结式的方阵. 定义 $\sigma_k=\det S_k$, 我们将证明: 若 f,g 是首一多项式, 则

$$\sigma_k(f,g)=(-1)^{(n-k)(m-k)}\rho^{m-k}\sigma_k(g,r),$$

其中 $f=gq+\rho r$ 是由带余除法得出的, r 是次数小于 $\deg(g)$ 的首一多项式. 事实上, 记 f,g,q,r 的系数为 f_j,g_j,q_j,r_j, 则 $f=gq+\rho r$ 改写如下:

$$\begin{pmatrix} 1 \\ f_{n-1} \\ \vdots \\ f_0 \end{pmatrix}-\begin{pmatrix} 1 & & & \\ g_{m-1} & 1 & & \\ \vdots & & \ddots & \\ g_0 & & & 1 \\ & \ddots & & \\ & & \ddots & \vdots \\ & & & g_0 \end{pmatrix}=\begin{pmatrix} 0 \\ \vdots \\ 0 \\ \rho r_d \\ \vdots \\ \rho r_0 \end{pmatrix}. \tag{11.25}$$

而 $S_k(f,g)\in\mathbb{K}^{(n+m-2k)\times(n+m-2k)}$ 的第一列为

$$(1,f_{n-1},\cdots,f_{2k-m+1})^{\mathrm{T}}, \tag{11.26}$$

(11.25) 式左端第 2 个式子的列通过添加一些零或者截去一部分, 可以使其长度变为 $n+m-2k$, 如此之后, 它就是 $S_n(f,g)$ 右半部分的列的线性组合. 因此 $(0,\cdots,0,\rho r_d,\cdots,\rho r_{2k-m+1})^{\mathrm{T}}$ 是 $S_k(f,g)$ 的一个线性组合. 我们可以用它代替 $S_k(f,g)$ 中的列 (11.26), 这并不改变其行列式的值. 类似地, 可以用对应的 ρr_j 的列替换 $S_k(f,g)$ 中的其他 f_j 的列. 其次, 我们将 ρr_j 的列移到矩阵右边, 这改变了行

列式的符号 $(n-k)(m-k)$ 次. 总之, 我们有

$$
\begin{aligned}
\sigma_k(f,g) &= \det S_k(f,g) \\
&= (-1)^{(n-k)\times(m-k)} \begin{pmatrix}
1 & & & & & \\
g_{m-1} & \ddots & & & & \\
\vdots & & 1 & \rho r_d & \vdots & \ddots \\
\vdots & & \vdots & \vdots & & \rho r_1 \\
\vdots & & \vdots & \vdots & & \vdots \\
g_{2k-n+1} & & g_k & \rho r_{2k-m+1} & \cdots & \rho r_k
\end{pmatrix}.
\end{aligned}
$$

上述右端矩阵具有以下形式:

$$
\begin{pmatrix} D & 0 \\ * & S_n(g,\rho r) \end{pmatrix},
$$

此处 D 是 $(n-d)\times(n-d)$ 的下三角阵, 其对角线元素均为 1, 故

$$
\sigma_k(f,g) = (-1)^{(n-k)(m-k)}\sigma_k(g,\rho r) = (-1)^{(n-k)(m-k)}\rho^{m-k}\sigma_k(g,r), \qquad (11.27)
$$

由 (11.27) 式, 我们可以证明下列各式 (设 $f=\rho_0 r_0$, $g=\rho_1 r_1$, r_0, r_1 首一, 次数分别为 n, m, n_i 是余式首项系数), 对于 $0 \leqslant k \leqslant n_1 = \deg(g)$, 有

$$
\sigma_k = \deg S_k = \begin{cases} (-1)^{\tau_i}\rho_0^{m-n_i}\displaystyle\prod_{1\leqslant j\leqslant i}\rho_j^{n_{j-1}-n_i}, & 若\ k=n_i(对某个\ i\leqslant l), \\ 0, & 否则, \end{cases} \qquad (11.28)
$$

其中 $\tau_i = \sum_{1\leqslant j\leqslant i}(n_{j-1}-n_i)(n_j-n_i)$, 且子结式满足下述递归关系式 $(1\leqslant i<l)$:

$$
\sigma_m = \rho_1^{n-m},\ \sigma_{n_{i+1}} = (-1)^{(n_i-n_{i+1})(n-n_{i+1}+i+1)}\left(\rho_0\cdots\rho_{i+1}\right)^{n_i-n_{i+1}}\sigma_i. \qquad (11.29)
$$

首先证明 (11.28) 式. 由 S_k 的定义, 不难证明 σ_k 在第二种情形为零. 故可以假设 $k=n_i$(对某个 $i\leqslant l$). 显然这个 i 是惟一的, 从而 (11.28) 式中的表达式是有意义的. 对 $0\leqslant h\leqslant i$ 用归纳法到 h, 由 (11.27) 式, 有

$$
\sigma_k(r_0,r_1) = \sigma_k(r_h,r_{h+1})\prod_{1\leqslant j\leqslant h}(-1)^{(n_{j-1}-k)(n_j-k)}\rho_{j+1}^{n_j-1}.
$$

再应用归纳假设和 $\sigma_{n_i}(r_{i-1},r_i)=1$ 及 $\sigma_k(f,g)=\rho_0^{m-k}\rho_1^{n-k}\sigma_k(r_0,r_1)$ 就证得结论 (11.28). 而 (11.29) 式可由 (11.28) 式和计算 $\tau_{i+1}-\tau_i \pmod 2$ 得出.

现在, 引理的结论 (11.24) 式就可直接由 (11.28) 式中取 $k=0$ 得出 (此时 $n_l=0$). 而递归关系式 (11.29) 表明结式 $\sigma_0=\sigma_{n_l}$ 可由 $\mathbb{K}$ 由 $O(n^\mu\log n)$ 个运算算出. 引理证毕.

由引理 11.6, 立即有以下计算两个多项式的扩充的最大公因子的递归算法:

(算法 11.5) 计算 XGCD

输入: 首一多项式 $r_0,r_1\in\mathbb{K}[x]$, $\deg r_0>\deg r_1$, $k\in\mathbb{N}$, 向量 V 和 W.

输出: 整数 $h=\eta(k)\in\mathbb{N}$, 矩阵 $R_h\in\mathbb{K}[x]^{2\times 2}$, 使得 $(r_{h-1},r_h)^{\mathrm{T}}=R_h(r_0,r_1)^{\mathrm{T}}$, 向量 V 和 W 使 $V[i]=\rho_i$, $W[i]=n_i-n_{i+1}$.

Step 1: 若 $r_1=0$ 或 $k\leqslant\deg r_0-\deg r_1$, 则输出: $h=0, R_h=\begin{pmatrix}1&0\\0&1\end{pmatrix}$; V; W;

Step 2: $d=\lfloor k/2\rfloor$; $(\eta(d),R,V,W)=\mathrm{XGCD}(r_0|2d,r_1|(2d-(n_0-n_1)),d,V,W)$;

Step 3: $j=\eta(d)+1$, $\begin{pmatrix}r_{j-1}\\r_j\end{pmatrix}=R\begin{pmatrix}r_0\\r_1\end{pmatrix}$, $n_{j-1}=\deg r_{j-1}$, $n_j=\deg r_j$;

Step 4: 若 $r_j=0$ 或 $k\leqslant n_0-n_j$, 则输出: $h=\eta(d)$; $R_h=R$; V; W;

Step 5: $r_{j-1}=q_jr_j+\rho_{j+1}r_{j+1}$($r_{j+1}$ 是首一的);

Step 6: 若 $r_{j+1}=0$, 则输出 $h=j$; $R_h=R$; V; W;

Step 7: $n_{j+1}=\deg r_{j+1}$; $d^*=k-(n_0-n_j)$; 扩充 V 到 (V,ρ_{j+1}), 扩充 W 到 (W,n_j-n_{j+1});

Step 8: $(\eta(d^*),S,V^*,W^*)=\mathrm{XGCD}(r_j|2d^*,r_{j+1}|(2d^*-(n_j-n_{j+1})),d^*,V,W)$;

Step 9: 输出 $h=\eta(d^*)+j$; $R_h=S\begin{pmatrix}0&1\\\rho_{j+1}^{-1}&-q_j\rho_{j+1}^{-1}\end{pmatrix}R$; V; W.

上述算法计算了两个多项式 $r_0,r_1(\in\mathbb{K}[x], \deg r_0>\deg r_1)$ 的扩充 GCD, 以及向量 V 和 W, 使得 $V[i]=\rho_i\ (0\leqslant i\leqslant l)$, $W[i]=n_i-n_{j+1}\ (0\leqslant i\leqslant l-1)$. 在此基础上, 就可以利用引理 11.6 中的 (11.24) 和 (11.29) 式计算出结式, 从而可计算出范数, 这就是下面的算法, 不难看出该算法具有平方时间复杂度:

(算法 11.6) Norm(II)

输入: 单位 $\alpha=\sum_{i=0}^{n-1}a_i\theta^i\in\mathbb{Z}_q$, θ 是 n 次首一不可约多项式 $f(x)\in\mathbb{Z}_p[x]$ 的根, 精度 N.

输出: 范数 $N_{\mathbb{Q}_q/\mathbb{Q}_p}(\alpha)\pmod{p^N}$.

Step 1: $\beta = \sum_{i=0}^{n-1} a_i x^i \pmod{p^N}$; $d = \deg(\beta)$;

Step 2: $V[0] = 1; V[1] = a_d$; $W[0] = n - d$;

Step 3: $(l, R, V, W) = \text{XGCD}(f, \beta/a_d \bmod p^N, n, V, W)$;

Step 4: $r = 1$, $s = 1$;

Step 5: 对于 $i = 0$ 到 $\#W - 1$, 计算

$$S = SV[i+1] \bmod p^N;\ r \equiv rs^{W[i]} \pmod{p^N};$$

Step 6: 输出 r.

§11.4　改进的 AGM 算法

在本节中, 我们将结合 Satoh 算法和 AGM 算法中的想法, 给出一个改进的 AGM 算法, 它的运算速度将严格地快过 AGM 算法的原始情形, 这个想法是由 Gaudry 给出的.

前面我们给出了双变量的 AGM 序列 $(a_k, b_k)_{k=0}^{\infty}$, 它们满足 $a_k \equiv b_k \equiv 1 \pmod 4$, 且 $a_k \equiv b_k \pmod 8$. 现在从这个双变量的 AGM 序列, 可以如下定义一个单变量的 AGM 序列 $(\lambda_k)_{k=0}^{\infty}$, 其中 $\lambda_k = b_k/a_k$, 同时定义椭圆曲线的序列 E_{λ_k} 如下:

$$E_{\lambda_k}:\quad y^2 = x(x-1)(x-\lambda_k^2).$$

因为 $(a_{k+1}, b_{k+1}) = (\frac{a_k+b_k}{2}, \sqrt{a_k b_k})$, 故有以下递推关系:

$$\lambda_{k+1} = \frac{2\sqrt{\lambda_k}}{1+\lambda_k}. \tag{11.30}$$

在 §11.1 中, 我们证明了: 对一个通常的椭圆曲线 $\overline{E}: y^2 + xy = x^3 + \overline{c}$, $\overline{c} \in \mathbb{F}_q^*$, 双变量 AGM 序列可以从 $(a_0, b_0) = (1+4u, 1-4u)$ $(u \in \mathbb{Z}_q, u^2 \equiv \overline{c} \pmod 2)$ 开始. 然而, 我们不能应用这些初始值作为单变量 AGM 序列的初始值, 这是因为 (a_0, b_0) 仅仅是模 8 相等的, 这将导致 $\lambda_0 \equiv 1 \pmod 8$. 然而这个问题可以通过计算

$$(a_1, b_1) \equiv (1, 1-8u^2) \pmod{16}$$

并从

$$\lambda_1 \equiv 1 + 8u^2 \equiv 1 + 8c \pmod{16}$$

作为初始来解决, 其中 $c \in \mathbb{Z}_q$ 且 $c \equiv \overline{c} \pmod 2$.

与双变量 AGM 序列不同, 单变量 AGM 序列确实收敛

$$\lambda_k \equiv \lambda_{k+n} \pmod{2^{k+3}}.$$

另一方面, 我们在 §11.2 中已经证明了

$$\frac{b_{k+1}}{a_{k+1}} \equiv \Sigma\Big(\frac{b_k}{a_k}\Big) \pmod{2^{k+3}},$$

因此 $\lambda_{k+1} \equiv \Sigma(\lambda_k) \pmod{2^{k+3}}$. 将此式代入 (11.30) 式表明 λ_k 满足下面的方程:

$$\Sigma(Z)^2(1+Z)^2 - 4Z \equiv 0 \pmod{2^{k+3}}, \quad Z \equiv 1 + 8\Sigma^{k-1}(c) \pmod{16}.$$

令 $\Lambda_2(X,Y) = Y^2(1+X)^2 - 4X$, 则 λ_k 满足

$$\Lambda_2(X, \Sigma(X)) \equiv 0 \pmod{2^{k+3}}.$$

因为 $\Lambda_2(X,Y)$ 的两个偏导数模 2 均为零, 所以不能直接应用 $\Lambda_2(X,Y)$ 进行迭代. 于是我们做以下的变量替换: $X \leftarrow 1+8X$, $Y \leftarrow 1+8Y$, 从而获得改进的多项式

$$\widetilde{\Lambda}_2(X,Y) = (X + 2Y + 8XY)^2 + Y + 4XY,$$

令 γ_k 定义如下:

$$\lambda_k = 1 + 8\gamma_k,$$

则 γ_k 满足

$$\widetilde{\Lambda}_2(X, \Sigma(X)) \equiv 0 \pmod{2^k}, \qquad \gamma_k \equiv \sigma^{k-1}(c) \pmod 2.$$

$\widetilde{\Lambda}_2$ 的偏导数如下:

$$\frac{\partial \widetilde{\Lambda}_2}{\partial X} = 2(X + 2Y + 8XY)(1 + 8Y) + 4Y \equiv 0 \pmod 2,$$

$$\frac{\partial \widetilde{\Lambda}_2}{\partial Y} = (4(X + 2Y + 8XY) + 1)(1 + 4X) \equiv 1 \pmod 2.$$

在 §11.2 中, 我们证明了, 对于给定的双变量 AGM 序列 $(a_k, b_k)_{k=0}^{\infty}$, 可以通过下式计算 Frobenius 的迹:

$$\mathrm{Tr}\overline{F} \equiv t_k + \frac{q}{t_k} \pmod{2^{k+3}},$$

其中 $t_k = N_{\mathbb{Q}_q/\mathbb{Q}_p}(a_k/a_{k+1})$, 将 $a_{k+1} = \frac{a_k+b_k}{2}$, $\lambda_k = \frac{b_k}{a_k}$ 和 $\lambda_k = 1 + 8\gamma_k$ 代入 t_k 的表达式, 有

$$t_k = N_{\mathbb{Q}_q/\mathbb{Q}_p}\left(\frac{1}{1+4\gamma_k}\right).$$

将这个公式与计算 γ_k 的迭代算法及 §11.3 中计算范数的快速算法相结合，就有以下算法 (其中 w 是 CPU 字长的一个倍数，以使得 w 最接近 $\sqrt{n}$).

(算法 11.7) 改进的 AGM 算法

输入： 一条椭圆曲线 $\overline{E}: y^2+xy=x^3+c,\ c\in\mathbb{F}_q^*,\ j(\overline{E})=c^{-1}\notin\mathbb{F}_4,\ q=2^n$.

输出： $\#\overline{E}(\mathbb{F}_q)$.

Step 1: 令 $N=\lceil\frac{n}{2}\rceil+2$;

Step 2: 令 $y\equiv c \pmod 2$;

Step 3: 对 $i=2$ 到 w, 计算

3.1　$x\equiv\Sigma^{-1}(y) \pmod{2^i}$;

3.2　$y\equiv y-\widetilde{\Lambda}_2(x,y) \pmod{2^i}$;

Step 4: $x\equiv\Sigma^{-1}(y) \pmod{2^w}$;

Step 5:

$$D_x\equiv\frac{\partial\widetilde{\Lambda}_2(x,y)}{\partial X} \pmod{2^w},\qquad D_y\equiv\frac{\partial\widetilde{\Lambda}_2(x,y)}{\partial Y} \pmod{2^w},$$

Step 6: 对于 $m=1$ 到 $\lfloor\frac{N-1}{w}\rfloor$, 计算

6.1 $x\equiv\Sigma^{-1}(y) \pmod{2^{(m+1)w}}$;

6.2 $V\equiv\widetilde{\Lambda}_2(x,y) \pmod{2^{(m+1)w}}$;

6.3 对于 $i=0$ 到 $w-1$, 计算

6.3.1 $\Delta_y\equiv-2^{-(mw+i)}V \pmod 2$;

6.3.2 $\Delta_x\equiv\Sigma^{-1}(\Delta_y) \pmod{2^{w-i}}$;

6.3.3 $y\equiv y+2^{mw+i}\Delta_y \pmod{2^{(m+1)w}}$;

6.3.4 $V\equiv V+2^{(mw+i)}(D_x\Delta_x+D_y\Delta_y) \pmod{2^{(m+1)w}}$;

Step 7: 计算 $t=N_{\mathbb{Q}_q/\mathbb{Q}_2}(\frac{1}{1+4y})$ 到精度 N;

Step 8: 若 $t^2>2^{n+2}$, 令 $t=t-2^N$;

Step 9: 输出 $\#\overline{E}(\mathbb{F}_{2^n})=2^n+1-t$.

其中的 Step 7 要应用 "特征 2 的范数算法", 而对于 Σ^{-1} 的算法, 只要利用以下公式就能十分有效地进行：对于任意的 $x\in\mathbb{Z}_q$, 设 $x=\sum_{i=0}^{n-1}a_i\theta^i$, 其中 $\mathbb{Z}_q=\mathbb{Z}_p[\theta]$.

θ 是 $\mathbb{Z}_p$ 上的一个 n 次首一不可约多项式 $H(X)$ 的根, 且 $H(X) \bmod p$ 不可约, 则

$$\Sigma^{-1}\Big(\sum_{i=0}^{n-1} a_i\theta^i\Big) = \sum_{j=0}^{p-1}\Big(\sum_{0\leqslant pk+j<n}^{p-1} a_{pk+j}\theta^k\Big)C_j(\theta),$$

其中 $C_j(\theta) = \Sigma^{-1}(\theta^j) = \theta^{jp^{n-1}}$ 可以通过预运算计算出来. 在有了预运算后, 计算 $\Sigma^{-1}(z)$, $z \in \mathbb{Z}_q/(p^N\mathbb{Z}_p)$, 只需要 $\mathbb{Z}_q/(p^N\mathbb{Z}_q)$ 上 $p-1$ 个乘法即可完成.

不难看出, 在做了所有的预运算后, 改进的 AGM 算法需要的比特运算复杂度为 $O(n^{2.5+\varepsilon})$, 而所需存储空间为 $O(n^2)$. 但是通过更仔细的分析, 可以证明改进的 AGM 算法的运算复杂度小于原始的 AGM 算法的复杂度. 我们就不再具体分析, 有兴趣的读者可自行验证或参阅 Gaudry 的文章 [21].

§11.5 改进的 Satoh 算法

设 $\overline{E}$ 是 $\mathbb{F}_q$ 上一条通常的椭圆曲线, $q = p^n, j(\overline{E}) \notin \mathbb{F}_{p^2}, \mathbb{Q}_q$ 是 $\mathbb{Q}_p$ 的 n 次非分歧扩张, $\mathbb{Z}_q$ 是 $\mathbb{Q}_q$ 的赋值环, 于是

$$\mathbb{Q}_q = \mathbb{Q}_p[x]/\big(f(x)\big), \quad f(x) \in \mathbb{Z}_p[x],$$

其中 f 是一个 n 次不可约首一多项式且 $f(x) \bmod p$ 是 $\mathbb{F}_p[x]$ 中不可约多项式. 现在设 $\overline{\theta} \in \mathbb{F}_q$ 是 $\overline{f}(x)\,(:= f(x) \pmod p)$ 在 $\mathbb{F}_q$ 中的一个根, 使得 $\mathbb{F}_q = \mathbb{F}_p[\overline{\theta}]$, 因此 $\overline{\theta} \in \mathbb{F}_q$, 故 $\overline{\theta}$ 是一个 $(q-1)$ 次单位根. 令 θ 是 $\overline{\theta}$ 的 Teichmüller 提升, 即 θ 是 $\mathbb{Z}_q$ 中满足 $\overline{\theta} \equiv \theta \pmod p$ 的惟一的 $(q-1)$ 次单位根. 令 $m(x) \in \mathbb{Z}_p[x]$ 是 θ 的极小多项式. 注意到 $m(x) \equiv f(x) \pmod p$, 故也可以将 $\mathbb{Q}_q$ 表示为 $\mathbb{Q}_p[x]/\big(m(x)\big)$. 因为 $\Sigma(\theta) \equiv \theta^p \pmod p$ 且 $\Sigma(\theta)$ 是 $(q-1)$ 次单位根, 故有 $\Sigma(\theta) = \theta^p$. 于是可以十分有效地利用下式计算 Frobenius Σ:

$$\Sigma\Big(\sum_{i=0}^{n-1} a_i\theta^i\Big) = \sum_{i=0}^{n-1} a_i\theta^{ip},$$

此处需要将得到结果模去 $m(x)$. 为了提升 $j(\overline{E})$, 回顾一下 Lubin-Serre-Tate 关于典范提升的结果:

定理 11.1 (Lubin-Serre-Tate) *设 $\overline{E}$ 如上, Σ 是 $\mathbb{Z}_q$ 上的Frobenius, 而 $\Phi_p(X,Y)$ 是 p 次模多项式, 则方程组*

$$\begin{cases} \Phi_p\big(X, \Sigma(X)\big) = 0, \\ X \equiv j(\overline{E}) \pmod p \end{cases} \tag{11.31}$$

有惟一的解 $J \in \mathbb{Z}_q$, 它是 $\overline{E}$ 的典范提升 E 的 j 不变量.

因此, 为了求 $\overline{E}$ 的典范提升, 只要求出方程组 (11.31) 的解即可. 现假设有 $J \equiv j(E) \pmod{p^k}$, 而想计算 $j(E) = J + p^k e$. 将此代入 p 次模方程, 有

$$\begin{aligned} 0 &= \Phi_p\big(J + p^k e, \Sigma(J) + p^k \Sigma(e)\big) \\ &= \Phi_p\big(J, \Sigma(J)\big) + p^k e \frac{\partial \Phi_p}{\partial X}(J, \Sigma(J)) \\ &\quad + p^k \Sigma(e) \frac{\partial \Phi_p}{\partial Y}(J, \Sigma(J)) + p^{2k} r(e, \Sigma(e)), \end{aligned}$$

其中 $r(X,Y) \in \mathbb{Z}_q[X,Y]$. 因为 $\Phi_p\big(J, \Sigma(J)\big) \equiv 0 \pmod{p^k}$, 将上式除以 p^k 后得到关于 $e \pmod{p}$ 的关系式. 由于模方程满足 Kronecker 关系式

$$\Phi_p(X,Y) \equiv (X^p - Y)(X - Y^p) \pmod{p},$$

故

$$\frac{\partial \Phi_p}{\partial X}(J, \Sigma(J)) \equiv 0 \pmod{p}, \qquad \frac{\partial \Phi_p}{\partial Y}(J, \Sigma(J)) \not\equiv 0 \pmod{p},$$

注意到 $\Sigma(e) \equiv e^p \pmod{p}$, 有

$$e^p \equiv -\frac{\Phi_p(J, \Sigma(J))}{p^k \dfrac{\partial \Phi_p}{\partial Y}(J, \Sigma(J))} \pmod{p}.$$

取惟一的 p 次根 $e' \in \mathbb{F}_q$, 就得出 $j(E)$ 的一个更好的近似值, $j(E) \equiv J + p^k e' \pmod{p^{k+1}}$. 为了避免上面开 p 次方根, 考虑方程组

$$\begin{cases} \Phi_p\big(X, \Sigma^{-1}(X)\big) = 0, \\ X \equiv j(\overline{E}) \pmod{p}, \end{cases} \tag{11.32}$$

一个显然的事实是方程组 (11.32) 也给出 $\overline{E}$ 的典范提升的 j 不变量. 于是与上面过程类似, 将 $J + p^k e$ 代入方程组 (11.32), 可以得出

$$e \equiv -\frac{\Phi_p\big(\Sigma^{-1}(J), J\big)}{p^k \dfrac{\partial \Phi_p}{\partial Y}\big(\Sigma^{-1}(J), J\big)} \pmod{p}.$$

注意到 $\Phi_p\big(\Sigma^{-1}(J), J\big) \equiv 0 \pmod{p^k}$, 只要计算 $\frac{\partial \Phi_p}{\partial Y}\big(\Sigma^{-1}(J), J\big) \pmod{p}$ 的逆. 剩下的问题是计算 Σ^{-1}, 它可用

$$\Sigma^{-1}\Big(\sum_{i=0}^{n-1} a_i \theta^i\Big) = \sum_{j=0}^{p-1} \Big(\sum_{0 \leqslant pk+j < n} a_{pk+j} \theta^k\Big) C_j(\theta)$$

计算, 其中 $C_j(\theta)=\Sigma^{-1}(\theta^j)=\theta^{jp^{n-1}}$. $C_j(\theta)$ 可在预运算中得出. 于是我们可以有以下计算 $j(\overline{E})$ 的提升算法:

(算法 11.8) 提升 $j(\overline{E})$ 的原始算法

输入: 一个 j 不变量 $j\in\mathbb{F}_{p^n}\setminus\mathbb{F}_{p^2}$, 一个精度 N.

输出: $J\in\mathbb{Z}_q$, 使得 $J\equiv j \pmod p$ 且 $\Phi_p\big(\Sigma^{-1}(J),J\big)\equiv 0 \pmod{p^N}$.

Step 1: $d\equiv(\frac{\partial\Phi_p}{\partial Y}\big(\Sigma^{-1}(j),j\big))^{-1} \pmod p$;

Step 2: $y\equiv j \pmod p$;

Step 3: 对于 $i=2$ 到 N, 计算

3.1 $x\equiv\Sigma^{-1}(y) \pmod{p^i}$;

3.2 $y\equiv y-d\Phi_p(x,y) \pmod{p^i}$;

Step 4: 输出 y.

但这个算法中的主要问题是, 在每一步循环中, 它总是要重复计算 $\Phi_p(x,y)$, 尽管在第 $i+1$ 步中的 x 和 y 的值非常接近于第 i 步中相应的值. 为了提高以上算法的效率, 我们采用以下技巧, 假设已经对某个 w 计算出了 $y\equiv j(E) \pmod{p^w}$ 和 $x\equiv\Sigma^{-1}(y) \pmod{p^w}$. 注意到对 $m\geqslant 1$ 和 $i\geqslant 0$, 有

$$\begin{aligned}&\Phi_p\big(x+p^{mw+i}\Delta_x,y+p^{mw+i}\Delta_y\big)\\&\equiv\Phi_p(x,y)+p^{mw+i}\Big(\frac{\partial\Phi_p}{\partial X}(x,y)\Delta_x+\frac{\partial\Phi_p}{\partial Y}(x,y)\Delta_y\Big) \pmod{p^{(m+1)w}},\end{aligned}\tag{11.33}$$

从而只需知道 $\frac{\partial\Phi_p}{\partial X}(x,y)$ 和 $\frac{\partial\Phi_p}{\partial Y}(x,y) \pmod{p^w}$, 应用上式就可以从 $\Phi_p(x,y)$ 算出 $\Phi_p\big(x+p^{mw+i}\Delta_x,y+p^{mw+i}\Delta_y\big)$(只要 $i<w$). 因此, 我们可以如下改进 "提升 $j(\overline{E})$ 的原始算法": 首先, 应用 "提升 $j(\overline{E})$ 的原始算法" 计算出 $y\equiv j(E) \pmod{p^w}$, 然后利用 (11.33) 式来更新 $\Phi_p(x,y)$. 于是我们有

(算法 11.9) 提升 $j(\overline{E})$ 的算法

输入: 一个 j 不变量 $j\in\mathbb{F}_{p^n}\setminus\mathbb{F}_{p^2}$, 一个精度 N.

输出: $J\in\mathbb{Z}_q$, 使得 $J\equiv j \pmod p$ 且 $\Phi_p\big(\Sigma^{-1}(J),J\big)\equiv 0 \pmod{p^N}$.

Step 1: $d\equiv(\frac{\partial\Phi_p}{\partial Y}\big(\Sigma^{-1}(j),j\big))^{-1} \pmod p$;

Step 2: $y\equiv j \pmod p$;

Step 3: 对于 $i=2$ 到 w, 计算

3.1 $x\equiv\Sigma^{-1}(y) \pmod{p^i}$;

　3.2 $y \equiv y - d\Phi_p(x,y) \pmod{p^i}$;

Step 4: $x \equiv \Sigma^{-1}(y) \pmod{p^w}$;

Step 5: $D_x \equiv \frac{\partial \Phi_p}{\partial X}(x,y) \pmod{p^w}$;

Step 6: $D_y \equiv \frac{\partial \Phi_p}{\partial Y}(x,y) \pmod{p^w}$;

Step 7: 对于 $m = 1$ 到 $[\frac{N-1}{W}]$, 计算

　7.1 $x \equiv \Sigma^{-1}(y) \pmod{p^{(m+1)w}}$;

　7.2 $V \equiv \Phi_p(x,y) \pmod{p^{(m+1)w}}$;

　7.3 对 $i = 0$ 到 $w-1$, 计算

　　7.3.1 $\Delta_y \equiv -dp^{-(mw+i)}V \pmod{p}$;

　　7.3.2 $\Delta_x \equiv \Sigma^{-1}(\Delta_y) \pmod{p^{w-i}}$;

　　7.3.3 $y \equiv y + p^{mW+i}\Delta_y \pmod{p^{(m+1)w}}$;

　　7.3.4 $V \equiv V + p^{(mW+i)}\big(D_x\Delta_x + D_y\Delta_y\big) \pmod{p^{(m+1)w}}$;

Step 8: 输出 y.

Satoh 等人证明了, 对于 $w \simeq n^{\mu(1+\mu)}$ 和 $N \simeq n/2$, 上述提升 $j(\overline{E})$ 的算法时间复杂度为 $O\big(n^{2\mu+1/(1+\mu)}\big)$, 其中 μ 是一个常数, 使得两个 N 比特整数的乘法的时间复杂度为 $O(N^\mu)$. 例如：对普通乘法算法, $\mu = 2$, 对于 Karatsuba 乘法算法, $\mu = \log_2 3$, 对于 Schönhage 和 Strassen 乘法算法, $\mu = 1 + \varepsilon$, ε 为任意正实数. 但在实际计算时, 我们总取 w 是 CPU 字长的一个倍数.

现在, 我们有下面的图表：

$$
\begin{array}{ccccccccc}
E_0 & \xrightarrow{\widehat{\Sigma}_0} & E_1 & \xrightarrow{\widehat{\Sigma}_1} & \cdots & \longrightarrow & E_{n-1} & \xrightarrow{\widehat{\Sigma}_{n-1}} & E_0 \\
\pi\downarrow & & \pi\downarrow & & & & \pi\downarrow & & \pi\downarrow \\
\overline{E}_0 & \xrightarrow{\widehat{\sigma}_0} & \overline{E}_1 & \xrightarrow{\widehat{\sigma}_1} & \cdots & \longrightarrow & \overline{E}_{n-1} & \xrightarrow{\widehat{\sigma}_{n-1}} & \overline{E}_0
\end{array}
\tag{11.34}
$$

此处 E_i 是 $\overline{E}_i$ 的典范提升, $\widehat{\Sigma}_i$ 是 $\widehat{\sigma}_i$ 的提升, 而 $\widehat{\sigma}_i$ 是 σ_i 的对偶. 由于 $\overline{V} = \widehat{\sigma}_{n-1}\circ\cdots\circ\widehat{\sigma}_1\circ\widehat{\sigma}_0$ 是 q 次 Frobenius 的对偶, 故 $V = \widehat{\Sigma}_{n-1}\circ\cdots\circ\widehat{\Sigma}_1\circ\widehat{\Sigma}_0$ 是 $\mathbb{Z}_q$ 的 q 次 Frobenius 的对偶. 但一个自同态的迹与其对遇的迹相等, 故 $\mathrm{Tr}(\mathcal{F}) = \mathrm{Tr}(V) = c + q/c$, 其中 c 使得 $\mathcal{F}^*(\omega) = c\omega$, ω 是 E_0 上的不变微分. 令 c_i 定义如下：

$$\widehat{\Sigma}_i^*\big(\omega_{i+1}\big) = c_i\omega_i,$$

ω_i 是 E_i 上的不变微分则 $c = \prod_{0\leqslant i\leqslant n-1} c_i$. 因 $\overline{V}$ 是可分的, $c \not\equiv 0 \pmod{p}$, 故有

$$\mathrm{Tr}(\overline{F}) \equiv \prod_{0\leqslant i\leqslant n-1} c_i \pmod{q}.$$

但图表 (11.34) 中所有交换正方形是相互共轭的, 于是有

$$\mathrm{Tr}(\overline{F}) \equiv N_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0) \pmod q.$$

由前面的讨论, c_0 可由下面各式决定:

$$c_0^2 = \frac{j(E_0)-(504+12096z_0)v_0}{j(E_0)+240v_0},$$

$$v_0 = (12z_0^2+z_0)(j(E_0)-1728)-36,$$

$$z_0 = \frac{j(E_1)^2+195120j(E_1)+4095j(E_0)+660960000}{8\big(j(E_1)^2+j(E_1)\big(563760-512j(E_0)\big)+372735j(E_0)+8981280000\big)},$$

因此最后可得出以下算法:

(算法 11.10) 改进的 Satoh 算法 (或 SST 算法)

输入: 一条椭圆曲线 $\overline{E}: y^2+xy=x^3+a,\ a\in\mathbb{F}_{2^n}\setminus\mathbb{F}_4$.

输出: $\#\overline{E}(\mathbb{F}_{2^n})$.

Step 1: $N=[n/2]+13,\ N'=N-10$;

Step 2: $J=j(\overline{E})$ 的提升 (精度为 N); $J'=\Sigma^{-1}(J) \pmod{p^N}$;

Step 3: $Z\equiv\frac{J'^2+195120J'+4095J+660960000}{8\left(J'^2+J'(563760-512J)+372735J'+8981280000\right)} \pmod{p^{N'}}$;

Step 4: $V\equiv(12Z^2+Z)(J-1728)-36 \pmod{p^{N'}}$;

Step 5: $S=\left(\frac{J-(504+12096Z)V}{240V+J}\right)$ 的范数, 精度为 N';

Step 6: $c\equiv\mathrm{sqrt}(S) \pmod{2^{N'-1}}$;

Step 7: 若 $c\not\equiv 1 \pmod 4$, 则 $c\equiv -c \pmod{2^{N'-1}}$;

Step 8: 若 $c^2>2^{n+2}$, 则 $c=c-2^{N'-1}$;

Step 9: 输出 2^n-1-c.

可以证明, 上述算法的时间和空间复杂度分别为 $O(n^{2.5+\varepsilon})$ 和 $O(n^2)$. 上述算法是对特征为 2 的情形叙述的. 对于特征不为 2 的情形, 可类似写出相应的算法, 只是对应于 c_0 的公式不同而已. 具体的公式见 §10.3 和 §10.4 中的内容, 我们不在此详叙了, 有兴趣的读者可自行将相关的算法写出.

第十二章　Harley 算法

在本章中, 我们将介绍由 Harley 提出的一个计算 $\mathbb{F}_q$ 上通常的椭圆曲线点数的算法. 它是目前已知最快的算法, 其时间复杂度和空间复杂度分别为 $O(n^{2\mu}\log n)$ 和 $O(n^2)$(对于固定的小素数 p 及 $q=p^n$). 我们下面就来较详细地分析该算法.

§12.1　广义牛顿算法

在我们讲述改进的 Satoh 算法 (或曰 SST 算法) 时, 介绍了如何求解形式 $\Phi(X,\Sigma(X))=0$ 的方程 ($\Phi(X,Y)\in\mathbb{Z}_q[X,Y]$). 设 $x\in\mathbb{Z}_q$ 是 $\Phi(X,\Sigma(X))=0$ 的一个根. 假定已知 $x_m\equiv x \pmod{p^m}$, 定义 $\delta_m=(x-x_m)/p^m$, 则在 x_m 处的泰勒展开给出

$$\begin{aligned}0&=\Phi\big(x,\Sigma(x)\big)=\Phi\big(x_m+p^m\delta_m,\Sigma(x_m+p^m\delta_m)\big)\\&\equiv\Phi\big(x_m,\Sigma(x_m)\big)+p^m\big(\delta_m\Delta_x+\Sigma(\delta_m)\Delta_y\big)\pmod{p^{2m}},\end{aligned}\tag{12.1}$$

此处

$$\Delta_x\equiv\frac{\partial\Phi}{\partial X}\big(x_m,\Sigma(x_m)\big)\pmod{p^m},$$
$$\Delta_y\equiv\frac{\partial\Phi}{\partial Y}\big(x_m,\Sigma(x_m)\big)\pmod{p^m}.$$

这就表明 δ_m 是下述同余式的解:

$$-\frac{\Phi(x_m,\Sigma(x_m))}{p^m}\equiv\delta\Delta_x+\Sigma(\delta)\Delta_y(\bmod p^m).$$

令 $k=\mathrm{ord}_p(\Delta_y)$, 若 $\mathrm{ord}_p(\Delta_x)\geqslant k,\mathrm{ord}_p(\Phi(x_m,\Sigma(x_m))\geqslant k+m$ 且 $m>k$, 则有下述 Artin-Schreier 方程:

$$\begin{aligned}\Sigma(\delta)&\equiv a\delta+b\pmod{p^{m-k}},\\a&=-\Delta_x/\Delta_y,\\b&=-\Phi(x_m,\Sigma(x_m))/(p^m\Delta_y).\end{aligned}$$

因为 a 和 b 是整的, Σ 保持赋值, 故上述方程的任何解 $\delta'\in\mathbb{Z}_q$ 均满足 $\delta'\equiv\delta_m \pmod{p^{m-k}}$. 令 $x'_m=x_m+p^m\delta'$, 则 $x'_m\equiv x\pmod{p^{2m-k}}$ 且方程 (12.1) 表明 $\Phi(x'_m,\Sigma(x'_m))\equiv 0\pmod{p^{2m}}$. 又因为假定 $m>k$, 故

$$\mathrm{ord}_p\left(\frac{\partial\Phi}{\partial y}\big(x'_m,\Sigma(x'_m)\big)\right)=k,\qquad\mathrm{ord}_p\left(\frac{\partial\Phi}{\partial x}\big(x'_m,\Sigma(x'_m)\big)\right)\geqslant k,\tag{12.2}$$

因而可以重复相同的过程, 以找到达到任意精度的解 $x_N \equiv x \pmod{p^N}$.

将上述方案叙述成以下算法:

(算法 12.1) Gen_Newton_Lift

输入: 多项式 $\Phi(X,Y) \in \mathbb{Z}_q[X,Y]$, $x_0 \in \mathbb{Z}_q$, 使得 $\Phi\big(x_0, \Sigma(x_0)\big) \equiv 0 \pmod{p^{2k+1}}$, $k = \mathrm{ord}_p(\frac{\partial \Phi}{\partial Y}(x_0, \Sigma(x_0)))$, 精度 N.

输出: $x_N \in \mathbb{Z}_q$, 使得 $\Phi\big(x_N, \Sigma(x_N)\big) \equiv 0 \pmod{p^N}$ 且 $x_N \equiv x_0 \pmod{p^{k+1}}$.

Step 1: 若 $N \leqslant 2k+1$, 则 $x := x_0$;

Step 2: 否则

2.1 $N' = \lceil \frac{N}{2} \rceil + k$; $M = N' - k$;

2.2 $x' = \mathrm{Gen_Newton_Lift}(\Phi, x_0, N')$;

2.3 $y' = \Sigma(x') \pmod{p^N}$;

2.4 $V \equiv \Phi(x', y') \pmod{p^N}$;

2.5 $\Delta_x \equiv \frac{\partial \Phi}{\partial X}\big(x', y'\big) \pmod{p^{N'}}$;

2.6 $\Delta_y \equiv \frac{\partial \Phi}{\partial Y}\big(x', y'\big) \pmod{p^{N'}}$;

2.7 $a_n, b_n = \mathrm{Artin_Schreier_Root}(-\frac{\Delta_x}{\Delta_y}, -\frac{V}{p^M \Delta_y}, M, n)$;

2.8 $x = x' + p^M \frac{b_n}{1-a_n}$;

Step 3: 输出 x.

在第 2.7 步中, 用到了函数 Artin_Schreier__Root. 我们讨论如下: 设 $\mathbb{F}_q$ 是一有限域, $q = p^n$, 我们称形如

$$x^p - x + \alpha = 0, \qquad \alpha \in \mathbb{F}_q$$

的方程为一个 Artin-Schreier 方程. 而 Hilbert 的定理 90 是说, 该方程在 $\mathbb{F}_q$ 中有解当且仅当 $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = 0$. 因为 $\sigma(x) = x^p$, 我们可以将此类方程推广到 $\mathbb{Z}_q$ 上, 考虑如下形式的方程:

$$\Sigma(x) - ax - b = 0, \tag{12.3}$$

其中 Σ 是 σ 的提升, $a, b \in \mathbb{Z}_q$. 令 $a_1 = a$, $b_1 = b$, 归纳地定义 $\Sigma^k(x) = a_k x + b_k$, $2 \leqslant k \leqslant n$. 因 $\Sigma^n(x) = x$, 故得知方程 (12.3) 的惟一的解就是 $b_n/(1-a_n)$. 为了计算 $a_k, b_k \in \mathbb{Z}_q$, 我们应用下述公式:

$$\Sigma^{k+l}(x) = \Sigma^l(a_k x + b_k) = \Sigma^l(a_k)(a_l x + b_l) + \Sigma^l(b_k)$$

和所谓"平方 - 乘"算法. 从而有以下算法:

(算法 12.2) Artin_Schreier_Root

输入: $a, b \in \mathbb{Z}_q$, 幂次 m, 精度 N.

输出: $a_m, b_m \in \mathbb{Z}_q$, 使得 $\Sigma^m(x) \equiv a_m x + b_m \pmod{p^N}$, $\Sigma(x) \equiv ax+b \pmod{p^N}$.

Step 1: 若 $m = 1$, 则 $a_m \equiv a \pmod{p^N}$, $b_m \equiv b \pmod{p^N}$;

Step 2: 否则

　2.1 $m' = \lfloor \frac{m}{2} \rfloor$;

　2.2 $a_{m'}, b_{m'} = \text{Artin_Schreier_Root}(a, b, m', N)$;

　2.3 $a_m \equiv a_{m'} \Sigma^{m'}(a_{m'}) \pmod{p^N}$;

　2.4 $b_m \equiv b_{m'} \Sigma^{m'}(a_{m'}) + \Sigma^{m'}(b_{m'}) \pmod{p^N}$;

　2.5 若 $m \equiv 1 \pmod 2$, 则

　　2.5.1 $a_m \equiv a\Sigma(a_m) \pmod{p^N}$;

　　2.5.2 $b_m \equiv b\Sigma(a_m) + \Sigma(b_m) \pmod{p^N}$;

Step 3: 输出 a_m, b_m.

在前面的讨论中, 我们将 $\Phi(X, \Sigma(X)) = 0$ 的求解问题归结到下述形式方程的求解:

$$\alpha\Sigma(\delta) + \beta\delta + \gamma \equiv 0 \pmod{p^t}, \tag{12.4}$$

其中 $t = m - k > 0, \alpha, \beta, \gamma \in \mathbb{Z}_q$, α 是单位. 因为 Σ 保持赋值, 故方程 (12.4) 惟一决定 $\delta_m \bmod p^{m-k}$ 且 $x \equiv x_m + p^m \delta_m \pmod{p^{2m-k}}$. 假定有一个算法输出方程 (12.4) 的一个精度为 $t' = \lceil t/2 \rceil$ 的零点 $\delta_{t'}$, 则可以用相同的算法找到一个精度为 t 的零点 δ_t. 事实上, 将 $\delta_t = \delta_{t'} + p^{t'}\Delta_t$ 代入方程 (12.4), 有

$$\alpha\Sigma(\Delta_t) + \beta\Delta_t + \frac{\alpha\Sigma(\delta_{t'}) + \beta\delta_{t'} + \gamma}{p^{t'}} \equiv 0 \pmod{p^{t-t'}},$$

因为 $t - t' \leqslant t'$, 故可以应用同一个算法决定 $\Delta_t \bmod p^{t-t'}$, 从而决定 δ_t. 因此, 如果我们能够解决最基本的情形 (即找出方程 (12.4) 模 p 的解), 则立即可获得一个递归算法.

如果假定 $\text{ord}_p(\Delta_x) > \text{ord}(\Delta_y)$, 则 $\text{ord}_p(\beta) > 0$, 于是基本情形就是解方程 $\alpha\Sigma(\delta) + \gamma \equiv 0 \pmod p$. 因为 α 是单位, 这就惟一决定了 $\delta \bmod p$. 下面的算法 12.3 和算法 12.4 就分别解决了方程 (12.4) 和方程

$$\Phi(X, \Sigma(X)) = 0 \tag{12.5}$$

的求解问题.

(算法 12.3) Artin_Schreier_Root_II

输入: $\alpha, \beta, \gamma \in \mathbb{Z}_q$, $\alpha \in \mathbb{Z}_q^*$, $\mathrm{ord}_p(\beta) > 0$, 精度 N.

输出: $x \in \mathbb{Z}_q$, 使得 $\alpha\Sigma(x) + \beta x + \gamma \equiv 0 \pmod{p^N}$.

Step 1: 若 $N = 1$, 则 $x \equiv \big(-\gamma/\alpha\big)^{1/p} \pmod{p}$;

Step 2: 否则

2.1 $N' = \lceil \frac{N}{2} \rceil$; $M = N - N'$;

2.2 $x' = \text{Artin_Schreier_Root_II}(\alpha, \beta, \gamma, N')$;

2.3 $\gamma' \equiv \frac{\alpha\Sigma(x') + \beta x' + \gamma}{p^{N'}} \pmod{p^M}$;

2.4 $\Delta' = \text{Artin_Schreier_Root_II}(\alpha, \beta, \gamma', M)$;

2.5 $x \equiv x' + p^{N'}\Delta' \pmod{p^N}$;

Step 3: 输出 x.

(算法 12.4) Gen_Newton_Lift_II

输入: 多项式 $\Phi(X, Y) \in \mathbb{Z}_q$, $x_0 \in \mathbb{Z}_q$, 使得 $\Phi(x_0, \Sigma(x_0)) \equiv 0 \pmod{p^{2k+1}}$ 且 $\mathrm{ord}_p(\frac{\partial\Phi}{\partial X}(x_0, \Sigma(x_0))) > k$, $k = \mathrm{ord}_p(\frac{\partial\Phi}{\partial Y}(x_0, \Sigma(x_0)))$, 精度 N.

输出: $x_N \in \mathbb{Z}_q$, 使得 $\Phi(x_N, \Sigma(x_N)) \equiv 0 \pmod{p^N}$ 且 $x_N \equiv x_0 \pmod{p^{k+1}}$.

Step 1: 若 $N \leqslant 2k + 1$, 则 $x := x_0$;

Step 2: 否则

2.1 $N' = \lceil \frac{N}{2} \rceil + k$; $M = N' - k$;

2.2 $x' = \text{Gen_Newton_Lift_II}(\Phi, x_0, N')$;

2.3 $y' = \Sigma(x') \pmod{p^N}$;

2.4 $V \equiv \big(\Phi(x', y') \pmod{p^N}\big)/p^{N'} \pmod{p^M}$;

2.5 $\Delta_x \equiv (\frac{\partial\Phi}{\partial X}(x', y') \pmod{p^{N'}})/p^k \pmod{p^M}$;

2.6 $\Delta_y \equiv (\frac{\partial\Phi}{\partial Y}(x', y') \pmod{p^{N'}})/p^k \pmod{p^M}$;

2.7 $\Delta' = \text{Artin_Schreier_Root_II}(\Delta_y, \Delta_x, V, M)$;

2.8 $x \equiv x' + p^M\Delta' \pmod{p^N}$.

Step 3: 输出 x.

注记 12.1　条件 $\mathrm{ord}_p(\beta) > 0$ 意味着方程 (12.4) 的惟一解是整的. 事实上, 令 $b = -\beta/\alpha$, $c = -\gamma/\alpha$, 则 δ 也是方程 $\Sigma(\delta) = b\delta + c$ 的解. 重复应用 Σ 到此方程两端并注意到 $\Sigma^n(\delta) = \delta$, 就有

$$\delta = \frac{\sum_{i=0}^{n-1} \Sigma^i(c) \cdot \prod_{j=i+1}^{n-1} \Sigma^j(b)}{1 - N_{\mathbb{Q}_q/\mathbb{Q}_p}(b)}.$$

因 $\mathrm{ord}_p(b) = \mathrm{ord}_p(\beta) > 0$, 故 $1 - N_{\mathbb{Q}_q/\mathbb{Q}_p}(b)$ 是单位, 从而 $\delta \in \mathbb{Z}_q$.

对于算法 (12.3) 中第 1 步, 设 $\mathbb{F}_q = \mathbb{F}_p[\overline{\theta}]$, 则

$$\Big(\sum_{i=0}^{n-1} \overline{a}_i \overline{\theta}^i\Big)^{1/p} = \sum_{j=0}^{p-1} \Big(\sum_{0 \leqslant pk+j < n} \overline{a}_{pk+j} \overline{\theta}^k \Big) C_j(\overline{\theta}),$$

其中 $C_j(\overline{\theta}) = (\overline{\theta}^j)^{1/p} = \overline{\theta}^{jp^{n-1}}$. 这表明, 对 $\overline{z} \in \mathbb{F}_q$, 我们可以利用 $p-1$ 个 $\mathbb{F}_q$ 中乘法算出 $\overline{z}^{1/p}$. 另外, 我们也可以由 $\Phi(\Sigma^{-1}(X), X) = 0$ 代替方程 (12.5) 来避免开 p 次方根.

注记 12.2　算法 (12.3) 的复杂度由第 2.2 步和第 2.4 步中的递归步骤所决定. 若假设 $\mathbb{Z}_q$ 由域多项式的 Teichmüller 提升所表示, 则 $\mathbb{Z}_q/(p^N \mathbb{Z}_q)$ 中的 Frobenius 置换可在 $O((nN)^\mu)$ 个比特运算中完成. 设 $T(N)$ 是算法 (12.3) 的运算时间, 则有

$$T(N) \leqslant 2T(\lceil N/2 \rceil) + C((nN)^\mu),$$

其中 C 为常数. 上面的关系表明算法 (12.3) 的复杂度为 $O((nN)^\mu \log N)$, 于是算法 (12.3) 的复杂度为 $O((nN)^\mu \log N)$. 事实上, 在算法中, 只在第 2.2 步调用了它自己 1 次, 而精度则增长 2 倍, 故整个复杂度由第 2.7 步中的调用 Artin_Schreier_Root_II 所决定.

§12.2　提升域多项式与 Harley 算法

设 $\overline{\theta} \in \mathbb{F}_q = \mathbb{F}_p[\overline{\theta}]$, 而 $\theta \in \mathbb{Z}_q$ 是 $\overline{\theta}$ 的 Teichmüller 提升, 即 θ 是 $\mathbb{Z}_q$ 中惟一的 $q-1$ 次单位根, 使得 $\overline{\theta} \equiv \theta \pmod p$. 在前一节中, 我们假定 $\mathbb{Z}_q$ 表示为 $\mathbb{Z}_p[x]/(f(x))$, $f(x)$ 是 θ 的极小多项式. 因为 θ 是 $q-1$ 次单位根, 故有 $\Sigma(\theta) = \theta^p$ 且 $f(x) = \prod_{i=0}^{n-1}(x - \theta^{p^i})$. 令 ζ_p 是一个形式 p 次单位根, 则

$$f(x^p) = \prod_{i=0}^{p-1} f(\zeta_p^i x). \tag{12.6}$$

事实上, 这是由于对 $i = 0, 1, \cdots, n-1$, $f(x^p)$ 的每一个因子 $(x^p - \theta^{p^i})$ 都分裂为

$$(x - \theta^{p^i})(\zeta_p x - \theta^{p^i}) \cdots (\zeta_p^{p-1} x - \theta^{p^i}),$$

将 $f(x)$ 表示为 $f(x)=\sum_{i=0}^{p-1} f_i(x^p)x^i$, $f_i(x)\in\mathbb{Z}_q[x]$, 则方程 (12.6) 可改写为

$$f(x^p)=\prod_{j=0}^{p-1}\Big(\sum_{i=0}^{p-1}\zeta_p^{ij}f_i(x^p)x^i\Big)=\sum_{k=0}^{p-1}h_k\big(f_0(x^p),\cdots,f_{p-1}(x^p)\big)x^{pk},$$

其中 $h_k\in\mathbb{Z}_q[Y_0,\cdots,Y_{p-1}]$ 是 p 次齐次多项式. 这表明 $f(x)$ 满足

$$f(x)=\sum_{k=0}^{p-1}h_k\big(f_0(x),\cdots,f_{p-1}(x)\big)x^k. \tag{12.7}$$

表 12.1 给出了多项式 $h_k(Y_0,\cdots,Y_{p-1})$ 的一些例子:

表 12.1

$p=2$	$h_0=Y_0^2$ $h_1=-Y_1^2$
$p=3$	$h_0=Y_0^3$ $h_1=Y_1^3-3Y_0Y_1Y_2$ $h_2=Y_2^3$
$p=5$	$h_0=Y_0^5$ $h_1=Y_1^5+5(Y_0^2Y_1^2Y_3-Y_0^3Y_1Y_4-Y_0^3Y_2Y_3+Y_0^2Y_1Y_2^2-Y_0Y_1^3Y_2)$ $h_2=Y_2^5+5(Y_0^2Y_2Y_4^2+Y_0^2Y_3^2Y_4+Y_0Y_1^2Y_4^2-Y_0Y_1Y_2Y_3Y_4-Y_0Y_1Y_3^3$ $-Y_0Y_2^3Y_4+Y_0Y_2^2Y_3^2-Y_1^3Y_3Y_4+Y_1^2Y_2^2Y_4+Y_1^2Y_2Y_3^2-Y_1Y_2^3Y_3)$ $h_3=Y_3^5+5(Y_1Y_3^2Y_4^2-Y_0Y_3Y_4^3-Y_1Y_2Y_4^3+Y_2^2Y_3Y_4^2-Y_2Y_3^3Y_4)$ $h_4=Y_4^5$

假定已知 $f_t(x)\equiv f(x) \pmod{p^t}$, 令 $\delta_t=\frac{f(x)-f_t(x)}{p^t}$, 将 $f(x)=f_t(x)+p^t\delta_t(x)$ 代入 (12.7) 式, 就得出决定 $\delta_t(x) \bmod p^t$ 的一个关系式. 我们以 $p=2$ 为例, 则 (12.7) 式变为

$$\delta_t(x)-2\big(f_{t,0}(x)\delta_{t,0}(x)-xf_{t,1}(x)\delta_{t,1}(x)\big)+V_t(x)\equiv 0 \pmod{2^t}, \tag{12.8}$$

其中 $V_t(x)\equiv\big(f_t(x)-f_{t,0}(x)^2+xf_{t,1}(x)^2\big)/2^t \pmod{2^t}$. 假定我们已经有一个算法能算出 $\delta_t(x) \bmod p^{t'}$, $t'=\lceil t/2\rceil$, 则可以应用同样算法计算 $\delta_t(x) \bmod p^t$: 在 (12.8) 式中代入 $\delta_t=\delta_{t'}+p^{t'}\Delta_{t'}$, 将得出一个 mod $2^{t-t'}$ 的类似方程, 但 δ_t 被 $\Delta_{t'}$ 替代, 而 V_t 则被

$$\frac{V_t(x)+\delta_{t'}(x)-2\big(f_{t,0}(x)\delta_{t',0}(x)-xf_{t,1}(x)\delta_{t',1}(x)\big)}{2^{t'}} \pmod{2^{t-t'}}$$

所替代. 因为 $t-t' \leqslant t'$, 故可以应用相同的算法计算出 $\Delta_{t'}$, 从而可得出 δ_t. 这就得出了下面的算法 12.5 和算法 12.6.

(算法 12.5) Teichmüller_Field_Poly_Delta2

输入: 多项式 $f_0(x), f_1(x), V(x) \in \mathbb{Z}_p[x]$, 精度 N.

输出: 多项式 $\delta(x) \in \mathbb{Z}_p[x]$, 满足

$$\delta(x) - 2\big(f_0(x)\delta_0(x) - xf_1(x)\delta_1(x)\big) + V(x) \equiv 0 \pmod{2^N}.$$

Step 1: 若 $N=1$, 则 $\delta(x) \equiv -V(x) \pmod 2$;

Step 2: 否则

2.1 $N' = \lceil N/2 \rceil$;

2.2 $\delta'(x) :=$ Teichmüller_Field_Poly_Delta2 (f_0, f_1, V, N');

2.3 $\delta_0(x^2) \equiv \big(\delta'(x) + \delta'(-x)\big)/2 \pmod{2^N}$;

2.4 $\delta_1(x^2) \equiv \big(\delta'(x) - \delta'(-x)\big)/(2x) \pmod{2^N}$;

2.5 $V'(x) \equiv \frac{V(x)+\delta'(x)-2\left(f_0(x)\delta_0(x)-xf_1(x)\delta_1(x)\right)}{2^{N'}} \pmod{2^{N-N'}}$;

2.6 $\Delta(x) :\equiv$ Teichmüller_Field_Poly_Char2 $(f_0, f_1, V', N-N')$;

2.7 $\delta(x) \equiv \delta'(x) + 2^{N'}\Delta(x) \pmod{2^N}$;

Step 3: 输出 $\delta(x)$.

(算法 12.6) Teichmüller_Field_Poly_Char2

输入: n 次首一不可约多项式 $\overline{f}(x) \in \mathbb{F}_2[x]$, 精度 N.

输出: 精度为 N 的 Teichmüller 提升 $f(x) \in \mathbb{Z}_p[x]$, 即 $f(x)$ 满足

$$f(x) | x^{2^n-1} \pmod{2^N}, \text{ 且 } f(x) \equiv \overline{f}(x) \pmod 2.$$

Step 1: 若 $N=1$, 则 $f(x) \equiv \overline{f}(x) \pmod 2$;

Step 2: 否则

2.1 $N' = \lceil N/2 \rceil$;

2.2 $f'(x) :=$ Teichmüller_Field_Poly_Char2 $(\overline{f}, N')$;

2.3 $f_0(x^2) \equiv \big(f'(x) + f'(-x)\big)/2 \pmod{2^N}$;

2.4 $f_1(x^2) \equiv \big(f'(x) - f'(-x)\big)/(2x) \pmod{2^N}$;

2.5 $V(x) \equiv \big(f'(x) - f_0(x)^2 + xf_1(x)^2\big)/2^{N'} \pmod{2^{N-N'}}$;

2.6 $\delta(x) :=$ Teichmüller_Field_Poly_Delta2 $(f_0, f_1, V, N-N')$;

2.7 $f(x) \equiv f'(x) + 2^{N'}\delta(x) \pmod{2^N}$;

Step 3: 输出 $f(x)$.

注记 12.3 两个算法中第 2.3 步和第 2.4 步是对任一个多项式 $f(x)$, 找出满足 (12.7) 式 (mod 2^N) 的 h_0 和 h_1, 其余步骤意义都是显然的. 两个算法的复杂度可与算法 12.3 和算法 12.4 的复杂度分析类似进行, 其结果也是 $O((nN)^\mu \log N)$. 又显然这些算法的空间复杂度均为 $O(nN)$.

下面就来描述 Harley 算法. 因为在实际应用中, $p = 2$ 是最重要的情形, 所以我们就对此来详细说明, $p > 2$ 的情形可类似得出.

设

$$\overline{E}:\ y^2 + xy = x^3 + a, \quad a \in \mathbb{F}_{2^n}^*,\ j(\overline{E}) = a^{-2} \notin \mathbb{F}_4$$

是 $\mathbb{F}_{2^n}$ 上一条通常的椭圆曲线. 在改进的 AGM 算法中, 我们证明了, 如果 $\widetilde{\Lambda}_2(X, Y) = (X + 2Y + 8XY)^2 + Y + 4XY$, 而 γ_k 满足 $\widetilde{\Lambda}_2(\gamma_k, \Sigma(\gamma_k)) \equiv 0 \pmod{2^k}$, 则

$$\mathrm{Tr}\overline{F} \equiv t_k + \frac{q}{t_k} \pmod{2^{k+3}}, \quad t_k = N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{1}{1 + 4\gamma_k}\right).$$

只要域多项式的 Teichmüller 提升预先算出, 则方程 $\widetilde{\Lambda}_2(X, \Sigma(X)) = 0$ 可以利用算法 12.1 十分有效地求解, 然后, 再利用求范数 (Norm) 的算法可以十分有效地算出 t_k. 于是有以下算法:

(算法 12.7) Harley 算法

输入: 一条通常的椭圆曲线 $\overline{E}:\ y^2 + xy = x^3 + a$, $a \in \mathbb{F}_{2^n}^*$, $j(\overline{E}) = a^{-2} \notin \mathbb{F}_4$.

输出: $\#\overline{E}(\mathbb{F}_{2^n})$.

Step 1: $N = \lceil \frac{n}{2} \rceil + 2$;

Step 2: $f(x) =$ Teichmüller_Field_Poly_Char2 $(\overline{f}, N)$;

Step 3: $x \equiv a \pmod 2$;

Step 4: $x =$ Gen_Newton_Lift_II$(\widetilde{\Lambda}_2, x, N)$;

Step 5: $t =$ Norm_Char_2$(\frac{1}{1+4x}, N)$;

Step 6: 若 $t^2 > 2^{n+2}$, 则 $t = t - 2^N$;

Step 7: 输出 $2^n + 1 - t$.

其中的 Norm_Char_2 是计算 $\mathbb{Z}_{2^n}$ 上的一个元素的 Norm 的算法 11.6, 我们在上一章中曾专门讲过这个算法, 但是在实际计算中, 我们常常应用算法 11.4. 不难

看出, 如果应用算法 11.6, 则下面算法的时间复杂度就是 $O(n^{2\mu}\log n)$:

(算法 12.8) Norm_Char_2

输入: 一个元素 $a \in 1+2^v\mathbb{Z}_q$, $v \geqslant 2$, 精度 N.
输出: $N_{\mathbb{Q}_q/\mathbb{Q}_2}(a) \pmod{2^N}$.
Step 1: $s = \lfloor\sqrt{N}/2\rfloor$;
Step 2: $z = a^{2^s} - 1 \pmod{2^{N+s}}$;
Step 3: $w \equiv \log(1+z) \pmod{2^{N+s}}$;
Step 4: $w = 2^{-s}w \pmod{2^N}$;
Step 5: $u = 2^{-v}\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(w) \pmod{2^{N-v}}$;
Step 6: 输出 $\exp(4)^u \pmod{2^N}$.

其中第 3 步计算要用到 $\log(1+z)$ 的展开式

$$\log(1+z) = 2\sum_{j=1}^{\infty}\frac{\gamma^{2j-1}}{2j-1} \equiv 2\sum_{1\leqslant(v-1)(2j-1)<N-n}\frac{r^{2j-1}}{2j-1} \pmod{2^N},\quad \gamma = \frac{z}{2+z}.$$

而对于 $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(w)$, 要用到以下等式: 定义 $a_i \in \mathbb{Z}$, 使得

$$\log(a) \equiv \sum_{i=0}^{n-1} a_i\theta^i \pmod{2^N},$$

则

$$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}\big(\log(a)\big) \equiv \sum_{i=0}^{n-1} a_i \mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(\theta^i) \pmod{2^N},$$

而每个 $\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(\theta^i)(0\leqslant i\leqslant n-1)$ 可以通过牛顿公式预运算得出:

$$\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(\theta^i) + \sum_{j=1}^{i-1}\mathrm{Tr}_{\mathbb{Q}_q/\mathbb{Q}_2}(\theta^{i-j})f_{n-j} + if_{n-i} \equiv 0 \pmod{2^N}.$$

其中 $f(x) = \sum_{i=0}^{n} f_i x^i$ 是 $\overline{f}$ 的 Teichmüller 提升 (在算法 12.7 中第 2 步求得的).

因算法 12.7 中每一步的计算复杂度和空间复杂度分别不超过 $O(n^{2\mu}\log n)$ 和 $O(n^2)$, 故整个算法的时间复杂度和空间复杂度分别为 $O(n^{2\mu}\log n)$ 和 $O(n^2)$. 从而我们有以下定理:

定理 12.1 设 $\overline{E}$ 是 $\mathbb{F}_q$ 上 ($q=p^n$, p 是一固定的小素数) 一条通常椭圆曲线, 则存在一确定型算法计算有理点数 $\#\overline{E}(\mathbb{F}_q)$, 其时间复杂度为 $O\big(n^2(\log n)^2\log\log n\big)$, 存储空间要求为 $O(n^2)$.

第十三章　Kedlaya 算法

§13.1　de Rham 复形与上同调

一、de Rham 上同调

在这一节, 我们引入 de Rham 上同调并计算几个例子.

设 $x_1,\cdots,x_n$ 是 $\mathbb{R}^n$ 中的线性坐标, 定义 Ω^* 是 $\mathbb{R}$ 上由 $dx_1,\cdots,dx_n$ 生成的代数, 且具有以下关系:

$$\begin{cases}(dx_i)^2=0,\\ dx_idx_j=-dx_jdx_i, \quad i\neq j.\end{cases}$$

作为 $\mathbb{R}$ 上的向量空间, Ω^* 有一组基如下:

$$\begin{gathered}1,\quad dx_i,\quad dx_idx_j,\quad dx_idx_jdx_k,\quad \cdots,\quad dx_1dx_2\cdots dx_n,\\ i<j,\qquad i<j<k.\end{gathered}$$

我们定义 $\mathbb{R}^n$ 上的 $\mathbb{C}^\infty$ 微分形式是下述集合中的元素:

$$\Omega^*(\mathbb{R}^n)=\{\mathbb{R}^n\text{中的}\mathbb{C}^\infty\text{函数}\}\otimes_{\mathbb{R}}\Omega^*,$$

也就是说, ω 是一个微分形式, 当且仅当 ω 可惟一地写成以下形式:

$$\omega=\sum f_{i_1\cdots i_q}dx_{i_1}\cdots dx_{i_q},$$

其中 $f_{i_1\cdots i_q}$ 是 $\mathbb{C}^\infty$ 函数, 简记为

$$\omega=\sum f_Idx_I.$$

代数 $\Omega^*(\mathbb{R}^n)=\bigoplus_{q=0}^n\Omega^q(\mathbb{R}^n)$ 是自然的分次代数, 其中 $\Omega^q(\mathbb{R}^n)$ 由 $\mathbb{R}^n$ 上的 $\mathbb{C}^\infty$ q 形式组成, 它们之间存在微分算子

$$d:\quad \Omega^q(\mathbb{R}^n)\longrightarrow\Omega^{q+1}(\mathbb{R}^n).$$

(a) 若 $f\in\Omega^0(\mathbb{R}^n)$, 则 $df=\sum\frac{\partial f}{\partial x_i}dx_i$.

(b) 若 $\omega=\sum f_Idx_I$, 则 $d\omega=\sum df_Idx_I$.

例 13.1　若 $\omega=xdy$, 则 $d\omega=dxdy$.

这个 d 称作外微分, 它是 $\mathbb{R}^3$ 上多元微积分中所谓的梯度、旋度和散度的一个统一推广.

例 13.2　在 $\mathbb{R}^3$ 上, $\Omega^0(\mathbb{R}^3)$ 和 $\Omega^3(\mathbb{R}^3)$ 都是 $\mathbb{C}^\infty$ 函数域上的 1 维空间, 而 $\Omega^1(\mathbb{R}^3)$ 和 $\Omega^2(\mathbb{R}^3)$ 是 3 维的, 因此有以下结论:

$$\begin{array}{ccccc}
\{\text{函数}\} & \simeq & \{0\text{ 形式}\} & \simeq & \{3\text{ 形式}\}, \\
f & \leftrightarrow & f & \leftrightarrow & f dxdydz, \\
\{\text{向量场}\} & \simeq & \{1\text{ 形式}\} & \simeq & \{2\text{ 形式}\}, \\
X=(f_1,f_2,f_3) & \leftrightarrow & f_1dx+f_2dy+f_3dz & \leftrightarrow & f_1dydz-f_2dxdz+f_3dxdy.
\end{array}$$

而在函数而言,

$$df=\frac{\partial f}{\partial x}dx+\frac{\partial f}{\partial y}dy+\frac{\partial f}{\partial z}dz,$$

在 1 形式而言,

$$d\big(f_1dx+f_2dy+f_3dz\big)=\left(\frac{\partial f_3}{\partial y}-\frac{\partial f_2}{\partial z}\right)dydz-\left(\frac{\partial f_1}{\partial z}-\frac{\partial f_3}{\partial x}\right)dxdz+\left(\frac{\partial f_2}{\partial x}-\frac{\partial f_1}{\partial y}\right)dxdy.$$

在 2 形式而言,

$$d\big(f_1dydz-f_2dxdz+f_3dxdy\big)=\left(\frac{\partial f_1}{\partial x}+\frac{\partial f_2}{\partial y}+\frac{\partial f_3}{\partial z}\right)dxdydz.$$

总而言之

$$d(0\text{ 形式})=\text{梯度},\qquad d(1\text{ 形式})=\text{旋度},\qquad d(2\text{ 形式})=\text{散度}.$$

两个微分形式的楔积 (Wedge product): $\tau\wedge\omega$ 或 $\tau\cdot\omega$ 定义如下: 若 $\tau=\sum f_I dx_I$, $\omega=\sum g_J dx_J$, 则

$$\tau\wedge\omega=\sum f_I g_J dx_I dx_J.$$

显然有 $\tau\wedge\omega=(-1)^{\deg\tau\deg\omega}\omega\wedge\tau$.

定理 13.1　d 是一个反导数, 即

$$d(\tau\cdot\omega)=(d\tau)\cdot\omega+(-1)^{\deg\tau}\tau\cdot d\omega.$$

证明　由线性性, 只要对

$$\tau=f_I dx_I,\omega=g_J dx_J$$

验证即可. 但此时

$$\begin{aligned} d(\tau\cdot\omega) &= d(f_I g_I)dx_I dx_J \\ &= (df_I)g_J dx_I dx_J + f_I dg_J dx_I dx_J \\ &= (d\tau)\cdot\omega + (-1)^{\deg\tau}\tau\cdot d\omega. \end{aligned}$$

证毕.

定理 13.2 $d^2=0$.

证明 这可由以下事实得出：混合偏导数相等. 对函数而言,

$$d^2 f = d\left(\sum_i \frac{\partial f}{\partial x_i}dx_i\right) = \sum_{i,j}\frac{\partial^2 f}{\partial x_j \partial x_i}dx_j dx_i$$

此处 $\frac{\partial^2 f}{\partial x_j \partial x_i} = \frac{\partial^2 f}{\partial x_i \partial x_j}$, 但 $dx_j dx_i = -dx_i dx_j$, 因此 $d^2 f = 0$. 对形式而言, 若 $\omega = f_I dx_I$, 则

$$\begin{aligned} d^2\omega &= d^2(f_I dx_I) = d(df_I dx_I) \\ &= d(df)\cdot dx_I + (-1)^{\deg(df_I)}df_I d^2 x_I = 0. \end{aligned}$$

证毕.

我们称 $(\Omega^*(\mathbb{R}^n), d)$ 为 $\mathbb{R}^n$ 上的 de Rham 复形, d 的核称为闭形式 (closed forms), 而 d 的像称为正合形式 (exact forms).

注意到寻找一类闭形式等价于寻找某类微分方程的解. 例如, 寻找一个闭的 1 形式 $fdx+gdy$(在 $\mathbb{R}^2$ 上), 就转化为解微分方程 $\frac{\partial g}{\partial x}-\frac{\partial f}{\partial y}=0$.

由定理 13.2 知, 正合形式一定是闭形式, 这些相应于平凡的或者说我们不感兴趣的解. 因此, 对我们感兴趣的解的一个自然的度量是下面的 de Rham 上同调:

定义 13.1 *$\mathbb{R}^n$ 的 q 次 de Rham 上同调是向量空间*

$$H^q_{DR}(\mathbb{R}^n) = \frac{\{\text{闭 } q \text{ 形式}\}}{\{\text{正合 } q \text{ 形式}\}} \qquad (\text{商空间}).$$

对于一个闭形式 ω, 记它所在的上同调类为 $[\omega]$. 于是 ω 是一个正合 q 形式当且仅当 $[\omega]=0$ (作为 $H^q_{DR}(\mathbb{R}^n)$ 中元素).

注意到我们的所有定义对 $\mathbb{R}^n$ 中任何一个开集 U 也是完全可以的, 例如

$$\Omega^*(U) = \{U\text{上的 } \mathbb{C}^\infty \text{ 函数}\} \otimes_{\mathbb{R}} \Omega^*,$$

因此, 也可以考虑 U 的 de Rham 上同调 $H^q_{DR}(U)$.

例 13.3　(a) $n=0$,

$$H_{DR}^q(\text{Point})=\begin{cases}\mathbb{R}, & q=0,\\ 0, & q>0.\end{cases}$$

(b) $n=1$, 因为 $(\ker d)\cap\Omega^0(\mathbb{R}^1)$ 是常数函数, 故 $H_{DR}^0(\mathbb{R})=\mathbb{R}$. 在 $\Omega^1(\mathbb{R}^1)$ 上, $\ker d$ 是所有 1 形式. 而若 $\omega=g(x)dx$ 是一个 1 形式, 取

$$f=\int_0^x g(u)du,$$

则 $df=g(x)dx$, 故 $\mathbb{R}^1$ 上每个 1 形式都是正合的, 故 $H_{DR}^1(\mathbb{R}^1)=0$.

(c) 设 U 是 $\mathbb{R}^1$ 上 m 个不相交开区间的并, 则

$$H_{DR}^0(U)=\mathbb{R}^m,\qquad H_{DR}^1(U)=0.$$

(d) 一般地

$$H^*(\mathbb{R}^n)=\begin{cases}\mathbb{R}, & *=0,\\ 0, & \text{否则}.\end{cases}$$

这个结果称为 Poincare 引理. 我们将不给出其证明, 有兴趣的读者可参考某些标准的微分流形的教材.

de Rham 复形是所谓微分复形的一个例子. 下面给出关于微分复形的定义和某些基本结果:

向量空间的直和 $C=\bigoplus_{q\in\mathbb{Z}}C^q$ 称作一个微分复形, 如果存在一个同态

$$\cdots\longrightarrow C^{q-1}\xrightarrow{d}C^q\xrightarrow{d}C^{q+1}\longrightarrow\cdots,$$

使得 $d^2=d\circ d=0$. d 称为复形 C 的微分算子, C 的上同调是向量空间的直和

$$H(C)=\bigoplus_{q\in\mathbb{Z}}H^q(C),$$

其中

$$H^q(C)=(\ker d\cap C^q)/(\text{im }d\cap C^q),$$

此处 $\ker d$ 是 d 的核, $\text{im}\, d$ 是 d 的像.

两个微分复形 A 和 B 之间的映射 $f:A\to B$ 称作一个链映射, 如果 f 与 A 和 B 的微分算子交换 $f\circ d_A=d_B\circ f$, 即下列图表交换:

$$\begin{array}{ccccccccc}\cdots & \longrightarrow & A^{q-1} & \xrightarrow{d_A} & A^q & \xrightarrow{d_A} & A^{q+1} & \longrightarrow & \cdots\\ & & \downarrow f & & \downarrow f & & \downarrow f & & \\ \cdots & \longrightarrow & B^{q-1} & \xrightarrow[d_B]{} & B^q & \xrightarrow[d_B]{} & B^{q+1} & \longrightarrow & \cdots\end{array}$$

我们称一个向量空间的序列

$$\cdots \longrightarrow V_{i-1} \xrightarrow{f_{i-1}} V_i \xrightarrow{f_i} V_{i+1} \longrightarrow \cdots$$

是正合的, 如果对所有的 i, 有 $\ker f_i = \operatorname{im} f_{i-1}$. 如下形式的正合序列:

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

称为一个短正合序列.

给定一个微分复形的短正合列

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0,$$

其中 f 和 g 是链映射, 存在一个上同调的长正合列

$$\begin{array}{cccccccc} H^{q-1}(A) & \longrightarrow & H^{q-1}(B) & \longrightarrow & H^{q-1}(C) & \longrightarrow \\ H^q(A) & \xrightarrow{f^*} & H^q(B) & \xrightarrow{g^*} & H^q(C) & \xrightarrow{\delta^*} \\ H^{q+1}(A) & \longrightarrow & H^{q+1}(B) & \longrightarrow & H^{q+1}(C), \end{array} \tag{13.1}$$

在这个序列中, f^* 和 g^* 是自然诱导出的映射. 而 $\delta^*[c]$, $c \in C^q$, 是如下获得的:

$$\begin{array}{ccccccccc} & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & A^{q+1} & \xrightarrow{f} & B^{q+1} & \xrightarrow{g} & C^{q+1} & \longrightarrow & 0 \\ & & \uparrow & & d\uparrow & & d\uparrow & & \\ 0 & \longrightarrow & A^q & \xrightarrow{f} & B^q & \xrightarrow{g} & C^q & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \end{array} \tag{13.2}$$

由于 g 是满的, 存在一个 $b \in B^q$, 使得 $g(b) = c$, 但

$$g(db) = d(gb) = dc = 0 \quad (\text{因为 } c \text{ 是闭形式}),$$

故 $db \in \ker g = \operatorname{im}(f)$, 从而存在 $a \in A^{q+1}$, 使得 $db = f(a)$. 易知这个 a 是闭形式, 于是定义

$$\delta^*[c] = [a] \in H^{q+1}(A).$$

一个简单的图表追踪表明 δ^* 的定义与 c 的选取无关, 并且易知序列 (13.1) 是正合的.

二、具有紧支集的 de Rham 上同调

前面关于 de Rham 上同调的构造稍加改造, 就可引入另一类重要的流形不变量 —— 具紧支集的 de Rham 上同调.

设 f 是一个拓扑空间 X 上的连续函数, 则 f 的支集 (支撑集) 定义如下:

$$\mathrm{Supp}(f) = \overline{\{p \in X \mid f(p) \neq 0\}}.$$

此外 $\overline{\{\ \}}$ 表示集合 $\{\ \}$ 的闭包. 现在令 $X = \mathbb{R}^n$, 考虑 $\mathbb{R}^n$ 上所有具有紧支集的 $\mathbb{C}^\infty$ 函数的全体. 定义具有支集的 de Rham 复形 $\Omega_c^*(\mathbb{R}^n)$ 如下:

$$\Omega_c^*(\mathbb{R}^n) = \{\mathbb{R}^n\text{上具紧支集的}\mathbb{C}^\infty\text{函数}\} \otimes_{\mathbb{R}} \Omega^*.$$

这个复形的上同调记为 $H_c^*(\mathbb{R}^n)$.

例 13.4　(a)

$$H_c^*(\mathrm{point}) = \begin{cases} \mathbb{R}, & * = 0, \\ 0, & * \neq 0. \end{cases}$$

(b) $\mathbb{R}^1$ 的紧致上同调: 此时闭 0 形式为常数函数. 因为在 $\mathbb{R}^1$ 上没有常数函数具有紧支集, 故 $H_c^0(\mathbb{R}^1) = 0$. 为了计算 $H_c^1(\mathbb{R}^1)$, 考虑积分映射

$$\int_{\mathbb{R}^1} \Omega_c^1(\mathbb{R}^1) \to \mathbb{R}^1.$$

显然该映射是满的, 且在任何具有紧支集的正合 1 形式 df 上消失为 0. 因为如果 f 的支集位于 $[a, b]$ 内部, 则

$$\int_{\mathbb{R}^1} \frac{df}{dx} dx = \int_a^b \frac{df}{dx} dx = f(b) - f(a) = 0.$$

若 $g(x)dx \in \Omega_c^1(\mathbb{R}^1)$ 位在上述积分映射的核内, 则函数

$$f(x) = \int_{-\infty}^{x} g(u) du$$

将具有紧支集, 且 $df = g(x)dx$. 因此, $\int_{\mathbb{R}^1}$ 映射的核正好是正合形式, 于是

$$H_c^1(\mathbb{R}^1) = \frac{\Omega_c^1(\mathbb{R}^1)}{\ker(\int_{\mathbb{R}^1})} = \mathbb{R}^1.$$

(c) 更一般地,

$$H_c^*(\mathbb{R}^n) = \begin{cases} \mathbb{R}, & * = n, \\ 0, & * \neq n, \end{cases}$$

这个结果称为具有紧支集的上同调的 Poincare 引理.

以上的讨论和方法可以完全类似地推广到代数曲线上来, 有兴趣的读者可以参看有关的书籍 [22].

三、超椭圆曲线点数计算与 de Rham 上同调

设 $p \neq 2$ 为一个素数, $q = p^n$, $n \geqslant 1$. 设 $\overline{Q} \in \mathbb{F}_q[x]$ 是次数 $d = 2g+1$ 的首一多项式, $\overline{Q}$ 无重根, 即 $(\overline{Q}, \overline{Q}') = 1$. 记 $C_{\overline{Q}}$ 是 $\mathbb{F}_q$ 上仿射平面上的如下代数曲线:

$$y^2 = \overline{Q},$$

则条件 $(\overline{Q}, \overline{Q}') = 1$ 保证 $C_{\overline{Q}}$ 是非奇异的. $C_{\overline{Q}}$ 称为超椭圆曲线 (hyperelliptic curve). 当 $g = 1$ 时, $C_{\overline{Q}}$ 就是椭圆曲线. 对于 $\mathbb{F}_q$ 的每一个有限扩域 $\mathbb{F}_{q^m}$, 令

$$C_{\overline{Q}}(\mathbb{F}_{q^m}) = \{(a,b) \in \mathbb{F}_{q^m}^2 \mid b^2 = \overline{Q}(a)\}.$$

记 $\mathbb{F}$ 是 $\mathbb{F}_q$ 的代数闭包, 令

$$F: \mathbb{F} \to \mathbb{F}, \quad a \mapsto a^p$$

是 p 次 Frobenius 映射, 它是 $\mathbb{F}$ 的一个自同构. 置 $F_q := F^n$ 是 q 次 Frobenius 映射, 则对任意 $m \geqslant 1$, 有

$$\mathbb{F}_{q^m} = \{a \in \mathbb{F} \mid F_q^m(a) = a\}.$$

因为 $\overline{Q}$ 的系数属于 $\mathbb{F}_q$, F_q 诱导出 $C_{\overline{Q}}$ 上的一个映射:

$$F_q: \ C_{\overline{Q}}(\mathbb{F}) \to C_{\overline{Q}}(\mathbb{F}), \quad (a,b) \mapsto (F_q(a), F_q(b))$$

称为 $C_{\overline{Q}}$ 的 q 次 Frobenius 映射, 而 $C_{\overline{Q}}(\mathbb{F}_{q^m})$ 正好是 $C_{\overline{Q}}$ 上的 q 次 Frobenius 映射的固定点的集合.

令

$$C'_{\overline{Q}} := C_{\overline{Q}} - \{y \text{ 的零点}\},$$

则曲线 $C_{\overline{Q}}$ 和 $C'_{\overline{Q}}$ 有一个阶为 2 的自同构 l:

$$l: \ (a,b) \mapsto (a, -b).$$

令 $\overline{A} := \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{Q})$, 则 $\overline{A}$ 是曲线 $C'_{\overline{Q}}$ 的函数环. 注意在 $\overline{A}$ 中, y 和 $\overline{Q}$ 均是可逆的, 显然有

$$\begin{aligned}
\overline{A} &= (\mathbb{F}_q[x, \overline{Q}^{-1}])[y]/(y^2 - \overline{Q}) \\
&= \bigoplus_{i,j,k} \mathbb{F}_q x^i \overline{Q}^j y^k \quad (0 \leqslant i < d, j \in \mathbb{Z}, 0 \leqslant k < 2) \\
&= \bigoplus_{i,j} \mathbb{F}_q x^i y^j \quad (0 \leqslant i < d, j \in \mathbb{Z}).
\end{aligned}$$

令 $\mathbb{Z}_q := \mathbb{Z}_p[x]/(f)$, $\mathbb{Q}_q := \mathbb{Q}_p[x]/(f)$ 分别是 p-adic 整数环 $\mathbb{Z}_p$ 和 p-adic 数域 $\mathbb{Q}_p$ 的 n 次非分歧扩张, 其中 $f \in \mathbb{Z}_p[x]$ 是 $\mathbb{Z}_p$ 上的一个首一多项式, 使得 $f \bmod p$ 是 $\mathbb{F}_p$ 上 n 次不可约多项式. 置

$$A := \mathbb{Q}_q[x, y, y^{-1}]/(y^2 - Q) = \bigoplus_{i,j} \mathbb{Q}_q x^i y^j \quad (0 \leqslant i < d, j \in \mathbb{Z}),$$

其中 Q 是 $\overline{Q}$ 在 $\mathbb{Z}_q[x]$ 中的任意一个首一的提升.

A 是 $\mathbb{Q}_q$ 上代数曲线 C'_Q 的函数环, 它与提升 Q 的选取有关, 为了获得与 Q 的选取无关的环, 令

$$A^\infty := \left\{ \sum_{i,j} a_{ij} x^i y^j \mid a_{ij} \in \mathbb{Q}_q,\ |a_{ij}| \to 0\ (\text{当}|j| \to \infty\text{时}) \right\},$$

其中 $0 \leqslant i < d$, $j \in \mathbb{Z}$. A^∞ 中的元素是任意的序列 $f = \sum_{i,j} a_{ij} x^i y^j$, 使得对每个整数 k, 几乎所有 a_{ij} 都在 $p^k \mathbb{Z}_q$ 中, 或者

$$A^\infty = \mathbb{Q}_q \otimes_{\mathbb{Z}_q} A_+^\infty,$$

其中 A_+^∞ 是 $\mathbb{Z}_q[x, y, y^{-1}]/(y^2 - Q)$ 的 p-adic 完备化. 可以证明 A_+^∞(因而 A^∞) 与 Q 的选取无关.

环 A^∞ 是由以下级数构成的环:

$$f = \sum_{i,j} a_{ij} x^i y^j, \quad 0 \leqslant i < d, j \in \mathbb{Z},$$

其中 f 在集合 $S = \{(x, y) \in C_Q(\overline{\mathbb{Q}}_q) \mid |y| = 1\}$ 上收敛. 但是在 p-adic 情形下, 一个在闭单位圆上收敛的级数可能是不可积的 (正如在闭复单位圆上收敛的级数给出的函数虽然连续但可能不可微), 因此需要在 A^∞ 中选取具有更好性质的函数

$$A^\dagger := \left\{ \sum_{i,j} a_{ij} x^i y^j \in A^\infty \mid a_{ij} \in \mathbb{Q}_q,\ \lim_{|j| \to \infty} \inf v_p(a_{ij})/|j| > 0 \right\}.$$

$A^\dagger$ 中的元素称为超收敛级数. 可以证明 $A^\dagger$ 与 Q 的选取无关.

现在考虑 C'_Q 上的微分形式. 首先, C'_Q 上的函数是 A 中的元素, A 中每一个元素具有一个微分 df, 它们满足 Leibniz 法则: $d(fg) = fdg + gdf$ 且 $da = 0$(对任意 $a \in \mathbb{Q}_q$). 微分的全体形成一个 A 模, 而 d 是从 A 到 A 模的一个 $\mathbb{Q}_q$ 导数. 令 Ω 是由 df 生成的 A 模, 其中 $f \in A$, 但 f 是 x 与 y 的函数, 故 Ω 由 dx 与 dy 生成. 但 $y^2 = Q$ 意味着 $dy = \frac{Q'}{2y} dx$(注意 $2y$ 在 A 中可逆), 所以 Ω 实际上是维数 1 的自由 A 模, $Q'dx/2y$ 是一组 A 基,

$$\Omega = A \cdot \frac{dx}{2y}.$$

因此 C'_Q 的 de Rham 复形是

$$A \to A \cdot \frac{dx}{2y}, \; x^i y^j \mapsto (2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1})\frac{dx}{2y},$$

其中 A 是零次的, 而 $A(dx)/2y$ 是一次的, 从而 de Rham 上同调就是这个复形的同调群

$$H^0_{DR}(C'_Q) = \ker(d) = \{f \in A \,|\, df = 0\}, \quad H^1_{DR}(C'_Q) = \operatorname{coker}(d) = \left(A \cdot \frac{dx}{2y}\right)\Big/ dA.$$

我们可以类似地定义 $A^\dagger$ 的 de Rham 复形:

$$\begin{aligned} d: \quad & A^\dagger \quad \longrightarrow \quad A^\dagger \cdot \frac{dx}{2y}, \\ & \sum_{i,j} a_{ij} x^i y^j \quad \longmapsto \quad \sum_{i,j} a_{ij} d(x^i y^j) = \sum_{i,j} a_{ij}\left(2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1}\right)\frac{dx}{2y}. \end{aligned}$$

可以验证: 若 $\lim_{|j|\to\infty} \inf v_p(a_{ij})/|j| > 0$, 则类似的极限不等式对和式 $\sum_{i,j} a_{ij} \cdot \left(2ix^{i-1}y^{j+1} + jx^i Q' y^{j-1}\right)$ 中的系数也成立 (甚至 $\liminf$ 都不会变得更小), 因此可以类似地定义这个 de Rham 复形的上同调, 记之为 $H^i(C_{\overline{Q}})$, $i = 0, 1$.

为了叙述 de Rham 上同调与点数计算的关系, 我们需要回顾一下 Weil 定理:

定理 13.3 *存在一个次数为 $2g$ 的首一的整系数多项式 $P_{\overline{Q}}$, 它的复根 $\alpha_i (1 \leqslant i \leqslant 2g)$ 满足 $|\alpha_i| = q^{1/2}$, 并且可适当排序以使得 $\alpha_i \alpha_{g+i} = q$. 对每一个 $m \geqslant 1$, 有*

$$\# C_{\overline{Q}}(\mathbb{F}_{q^m}) = q^m - \sum_i \alpha_i^m, \tag{13.3}$$

而对于 $C_{\overline{Q}}$ 的Jacobi簇, 有

$$\# J_{\overline{Q}}(\mathbb{F}_q) = P_{\overline{Q}}(1). \tag{13.4}$$

因此, 要计算 $C_{\overline{Q}}$ 的有理点的数目, 只要能计算出多项式 $P_{\overline{Q}}$ 即可.

回忆曲线 $C'_{\overline{Q}}$ 上的 2 阶自同态 l:

$$l: \quad (a, b) \longmapsto (a, -b).$$

则 l 诱导出 $H^1(C'_{\overline{Q}})$ 上的自同构 l^*, 且 $H^1(C'_{\overline{Q}})$ 可分解为 l^* 的两个特征值为 1 和 -1 的特征空间的直和

$$H^1(C'_{\overline{Q}}) = H^1(C'_{\overline{Q}})^+ \bigoplus H^1(C'_{\overline{Q}})^-.$$

类似地, 有 $H^1_{DR}(C'_{\overline{Q}}) = H^1_{DR}(C'_{\overline{Q}})^+ \oplus H^1_{DR}(C'_{\overline{Q}})^-$. 另一方面, $C'_{\overline{Q}}$ 上的 Frobenius 映射

$$F_q: \quad C'_{\overline{Q}}(\mathbb{F}) \longrightarrow C'_{\overline{Q}}(\mathbb{F})$$

将诱导出对应的上同调之间的一个同态

$$F_q^*: \quad H^1(C'_{\overline{Q}}) \longrightarrow H^1(C'_{\overline{Q}}).$$

定理 13.4　$P_{\overline{Q}}$ 是 F_q^* 在 $H^1(C'_{\overline{Q}})^-$ 上的特征多项式.

定理 13.4 的证明超出了本书的范围，但我们指出，它可以由算术代数几何中的 Lefschetz 迹公式导出.

由定理 13.4，我们如果能找到 $H^1(C'_{\overline{Q}})^-$ 的一组基，并能够计算出 F_q^* 在这组基上的作用，则能获得 F_q^* 在向量空间 $H^1(C'_{\overline{Q}})^-$ 上的矩阵，从而得出该矩阵的特征多项式 $P_{\overline{Q}}$，再利用定理 13.3，就能计算出 $\#C_{\overline{Q}}(\mathbb{F}_q)$ 和 $\#J_{\overline{Q}}(\mathbb{F}_q)$. 于是，我们下面的任务就是：

(a) 找到 $H^1(C'_{\overline{Q}})^-$ 的一组清晰的基.

(b) 计算 F_q^* 在这组基上的作用，从而算出 F_q^* 的矩阵和特征多项式.

§13.2　上同调空间的基

由第一节的讨论知道，为了计算超椭圆曲线的有理点的个数，只要找出上同调空间上的一组清晰的基，并研究 Frobenius 在这组基上的作用即可. 这正是本节的主要任务.

定理 13.5　我们有 $H^0_{DR}(C'_Q) = \mathbb{Q}_q$. 而上同调类 $[x^i y^{-1}(dx)/y](0 \leqslant i \leqslant 2g)$ 形成 $H^1_{DR}(C'_Q)^+$ 的一组基，上同调类 $[x^i(dx)/y](0 \leqslant i < 2g)$ 形成 $H^1_{DR}(C'_Q)^-$ 的一组基.

证明　首先将 de Rham 复形分裂为 l 的两个特征空间之和. 回忆环 A 具有 $\mathbb{Q}_q$ 基 $x^i y^j, 0 \leqslant i < d, j \in \mathbb{Z}$，且 $lx = x, ly = -y$. 因此有 l 特征空间的如下分解：

$$A^+ = \bigoplus_{\substack{0\leqslant i<d\\ j\equiv 0 \pmod 2}} \mathbb{Q}_q x^i y^j = \bigoplus_{\substack{0\leqslant i<d\\ j\in\mathbb{Z}}} \mathbb{Q}_q x^i Q^j = \mathbb{Q}_q[x, Q^{-1}],$$

$$\Omega^+ = \bigoplus_{\substack{0\leqslant i<d\\ j\equiv 1 \pmod 2}} \mathbb{Q}_q x^i y^j \frac{dx}{2y} = \bigoplus_{\substack{0\leqslant i<d\\ j\equiv 1 \pmod 2}} \mathbb{Q}_q x^i Q^{(j-1)/2} dx = \mathbb{Q}_q[x, Q^{-1}]dx,$$

$$A^- = \bigoplus_{\substack{0\leqslant i<d\\ j\equiv 1 \pmod 2}} \mathbb{Q}_q x^i y^j,$$

$$\Omega^- = \bigoplus_{\substack{0\leqslant i<d\\ j\equiv 0 \pmod 2}} \mathbb{Q}_q x^i y^j \frac{dx}{2y}.$$

首先研究 “+” 空间. 事实上，这一部分正好是环 $\mathbb{Q}_q[x, Q^{-1}]$ 的 de Rham 复形，即曲线

$\mathbb{A}^1$-{Q的零点} 的 de Rham 复形. 由此不难证明 $H^0_{DR}(C'_Q)^+ = \mathbb{Q}_q$ 且 $x^iQ^{-1}dx, 0 \leqslant i < d$, 形成 $H^1_{DR}(C'_Q)^+$ 的一组基.

其次, 研究 "$-$" 空间. 我们在单项式 $x^iy^j(0 \leqslant i < d, j \in \mathbb{Z})$ 中引进先 j 后 i 的字典序, 即若 $j_1 > j_2$, 则 $x^iy^{j_1}$ 高于 $x^{i'}y^{j_2}$; 若 $j_1 = j_2$, 则当且仅当 $i > i'$ 时, $x^iy^{j_1}$ 高于 $x^{i'}y^{j_2}$. 对 $0 \leqslant i < d$, 考虑 $\mathbb{Q}_q[x]$ 中如下带余除法:

$$x^iQ' = a_iQ + b_i, \quad \deg(b_i) < d.$$

我们有 $a_0 = 0$, $b_0 = Q'$. 对于 $1 \leqslant i < d$, 有 $a_i = dx^{i-1} + \cdots$, 因此 $\deg(a_i) = i - 1$. 则有

$$d: \ x^iy^j \mapsto (2ix^{i-1}y^{j+1} + jx^iQ'y^{j-1})\frac{dx}{2y} = (2ix^{i-1}y^{j+1} + ja_iy^{j+1} + jb_iy^{j-1})\frac{dx}{2y}.$$

对于 $0 \leqslant i < d$ 且 $j \equiv 1 \pmod 2$, $d(x^iy^j)$ 的最高次单项式为

$$\begin{cases} x^{i-1}y^{j+1}, & \text{如果 } 1 \leqslant i < d, \\ x^{d-1}y^{j-1}, & \text{如果 } i = 0, \end{cases}$$

这是因为 $2i + jd \neq 0$ 且 $jd \neq 0$.

又因为 $(Q, Q') = 1$, 故在 $\mathbb{Q}_q[x]/(Q)$ 中的乘 Q' 映射是一个同构. 从而 $b_0, b_1, \cdots, b_{d-1}$ 形成 $\mathbb{Q}_q[x]_{<d} := \{f \in \mathbb{Q}_q[x] | \deg(f) < d\}$ 的一组 $\mathbb{Q}_q$ 基, 从而知道 $d(x^iy^j)$ 的最低次单项式具有形式 $x^ky^{j-1}, 0 \leqslant k < d$.

现在, 证明 $H^0_{DR}(C'_Q)^- = \ker(d: A^- \to \Omega^-) = 0$. 这可以从以下事实立即推出: 所有 $d(x^iy^j)(0 \leqslant i < d, j \equiv 1 \pmod 2)$, 都具有不同的最高次单项式, 因而 $d(x^iy^j)$ 是线性无关的.

剩下的任务是证明上同调类 $[x^i(dx)/y](0 \leqslant i < d-1)$ 形成 $H^1_{DR}(C'_Q)^- = \Omega^-/dA^-$ 的一组基. 首先证明这些元素是线性无关的. 因此假定存在 λ_k, 使得

$$\sum_{0 \leqslant k < d-1} \lambda_k[x^i(dx)/y] = [0],$$

即 $\sum_{0 \leqslant k < d-1} \lambda_k x^i(dx)/y \in dA^-$, 亦即存在 $\mu_{ij}(0 \leqslant i < d, j \equiv 1 \pmod 2)$, 使得几乎所有的 $\mu_{ij} = 0$ 且

$$\sum_{0 \leqslant k < d-1} \lambda_k x^k(dx)/y = \sum_{\substack{0 \leqslant i < d \\ j \equiv 1 \pmod 2}} \mu_{ij} d(x^iy^j) \neq 0.$$

由前面的讨论, 知 $d(x^iy^j)$ 最高次单项式是

$$\begin{cases} x^{i-1}y^{j+1}, & \text{如果 } 1 \leqslant i < d, \\ x^{d-1}y^{j-1}, & \text{如果 } i = 0, \end{cases}$$

与左边 $\sum\lambda_k x^k(dx)/y$ 相比较, 可知 $j=-1$(若 $1\leqslant i<d$) 或 $j=1$(若 $i=0$). 因此, 出现在右端和式 $\sum\mu_{ij}d(x^iy^j)$ 中的最高次单项式一定具有形式 x^iy^{-1} 或 y(按 $1\leqslant i<d$ 或 $i=0$). 但 y 是不能出现的, 因为 $dy=\frac{Q'dx}{2y}$, $\deg Q'=d-1$, 而此式在左边的和式 $\sum_{0\leqslant k<d-1}\lambda_k x^k(dx)/y$ 中不存在 (因 $k<d-1$), 所以出现在右端和式 $\sum\mu_{ij}d(x^iy^j)$ 中最高次单项式必具有形式 x^iy^{-1}. 另一方面, 由前面的讨论, $d(x^iy^j)$ 中的最低次单项式为 jb_iy^{j-1}, 由于 b_i 是线性无关的, 因此与左边和式 $\sum\lambda_k x^k(dx)/y$ 比较可知必有 $j=1$, 从而出现在右端和式 $\sum\mu_{ij}d(x^iy^j)$ 的最低次单项式必具有形式 x^iy, $0\leqslant i<d$. 这是一个矛盾. 因为按照我们规定的字典序, 应有 x^iy 高于 x^iy^{-1}(先 j 后 i), 所以右端必为零, 从而左端亦然. 但作为微分 $x^k(dx)/y$ $(0\leqslant k<d-1)$ 显然是线性无关的, 从而 $\lambda_k=0, 0\leqslant k<d-1$.

最后, 证明 $[x^i(dx)/y]$ 生成 $H^1_{DR}(C'_Q)^-=\Omega^-/dA^-$. 我们的方法是给出一个约化算法, 它将 Ω^- 中任意元素 $f(dx)/y$ 写成 dA^- 中一个元素与 $x^i(dx)/y$ 的一个线性组合之和. 现设 $f(dx)/y$ 被给定. 只要 f 具有一个单项 x^iy^j, 使得 $j<0$, 则如下计算: 令 x^iy^j 是 f 的最低次单项式, 应用 $d(x^ky^{j+1})$ 的惟一的线性组合 dg, 使得 $f(dx)/y-dg$ 没有单项式 x^my^n, $n=j$. 现在设 f 没有单项式 $x^iy^j(j<0)$. 设 f 具有单项式 $x^iy^j(j>0)$, 则如下计算: 令 x^iy^j 是 f 的最高次单项式, 设 x^ky^l 是一单项式, 使得 $d(x^ky^l)$ 具有最高次单项式 x^iy^j, 于是用 $f(dx)/y$ 减去 $d(x^ky^l)$ 的一个适当倍数代替 $f(dx)/y$, 从而可设 f 没有单项式 x^iy^j, $j>0$, 进而 f 没有形如 x^iy^j $(j\neq 0)$ 的单项式. 现在将 $f(dx)/y$ 减去 dy 的一个适当的倍数, 使得单项式 $x^{d-1}y$ 不出现在这个差中, 于是 $f(dx)/y$ 是 $x^i(dx)/y\,(0\leqslant i<d-1)$ 的一个线性组合. 事实上, 若 f 的最高次项为 x^σ, $\sigma\geqslant d-1=2g$, 则将 $f(dx)/y$ 减去 $d(x^{\sigma-2g}y)$ 的适当倍数, 即可将 f 的次数降低, 从而 $f(dx)/y$ 是 $x^i(dx)/y\,(0\leqslant i<d-1)$ 的一个线性组合加上 dA^- 中一个元素, 这就完成了证明.

上述定理证明的最后部分 (约化算法) 可重写如下 (写 $\tau=\frac{1}{y^2}$):

(算法 13.1) Reduction 算法

Step 1: 对于一个多项式 $Q_k(x)$, 有

$$Q_k(x)\tau^k=(\alpha_k(x)Q(x)+\beta_k(x))\tau^k=\alpha_k(x)\tau^{k-1}+\beta_k(x)\tau^k,$$

此处 $Q_k(x)=\alpha_k(x)Q(x)+\beta_k(x)$, $\deg\beta_k(x)<\deg Q(x)$, 因此可以假定 $Q_k(x)$ 的次数最多为 $2g=d-1$.

Step 2: 对于一个多项式 $Q_k(x)$, $k\geqslant 1$, 设 $u(x)$ 和 $v(x)$, 使得 $Q_k(x)=u(x)Q(x)+$

$v(x)Q'(x)$(因 $(Q,Q')=1$, 这样的 $u(x),v(x)$ 存在), 应用正合微分 $d\big(v(x)/y^{2k-1}\big)$, 有

$$Q_k(x)\tau^k\frac{dx}{y}\equiv\left(u(x)+\frac{2}{2k-1}v'(x)\right)\tau^{k-1}\frac{dx}{y},$$

其中 "≡" 表示左右两边差一个正合微分.

Step 3: 在表达式 $Q_k(x)\frac{dx}{y}$ 中, 我们能够应用正合微分 $d(x^{\sigma-2g}y)$(其中 $\sigma=\deg Q_k\geqslant 2g$), 将 $Q_k(x)$ 的次数降低, 这是因为

$$\begin{aligned}d(x^{\sigma-2g}y)&=(\sigma-2g)x^{\sigma-2g-1}ydx+x^{\sigma-2g}\frac{Q'dx}{y}\\&=\big(2(\sigma-2g)x^{\sigma-2g-1}Q(x)+x^{\sigma-2g}Q'\big)\frac{dx}{2y}\end{aligned}$$

的次数为 σ, 首项系数 $=2(\sigma-2g)+2g+1=2\sigma-2g+1\neq 0$.

现在, 我们有向量空间

$$H^1_{DR}(C'_Q)^-=\bigoplus_{0\leqslant i<d-1}\mathbb{Q}_q x^i(dx)/y.$$

但事实上还需要向量空间 $H^1(C'_{\overline{Q}})^-$ 的一组基.

定理 13.6 *上同调类元素 $[x^i(dx)/y](0\leqslant i<d-1)$ 形成 $H^1(C'_{\overline{Q}})^-$ 的一组基.*

证明 首先, 可以与定理 13.5 的证明中完全类似地证明上同调类 $[x^i(dx)/y]$ $(0\leqslant i<d-1)$ 是线性无关的, 所以只需要证明它们还生成整个空间 $H^1(C'_{\overline{Q}})^-$. 因此, 设 $\sum_m a_my^m(dx)/y$ 是 $A^\dagger\cdot\frac{dx}{y}$ 中一个元素, 其中 $a_m\in\mathbb{Q}_q[x]$ 且 $\deg(a_m)<d$, 乘上 p 的一个适当幂次, 有 $a_m\in\mathbb{Z}_q[x]$(对所有 m). 对每一个 $m\neq 0$, 下面的引理 13.1 和 13.2 将给出一个 $b_m\in\mathbb{Q}_q[x]$ 和 $f_m\in A^-$, 使得 $a_my^m(dx)/y=b_m(dx)/y+df_m$ 且 $\deg(b_m)<d-1$, 由定义, 存在一个 $\varepsilon>0$ 及整数 m_0, 使得 a_m 被 $p^{\lfloor\varepsilon|m|\rfloor}$ 整除 (只要 $|m|>m_0$). 因此, 在 $A^\dagger\cdot\frac{dx}{y}$ 中有

$$\sum a_my^m\frac{dx}{y}=a_0(dx)/y+\bigg(\sum_{m\neq 0}b_m\bigg)(dx)/y+d\bigg(\sum_m f_m\bigg).$$

对于 $a_0=a_{0,d-1}x^{d-1}$, 应用以下恒等式:

$$dy=Q'\frac{dx}{2y}=\big(dx^{d-1}+\cdots\big)\frac{dx}{2y},$$

故减去 dy 的一个适当倍数, 可设 a_0 的次数小于 $d-1$, 从而 $[x^i(dx)/y](0\leqslant i<d-1)$ 生成了整个空间 $H^1(C'_{\overline{Q}})^-$. 这就完成了定理的证明.

引理 13.1　设 $\omega = ay^{-m}(dx)/y$, $m > 0$, $m \equiv 0 \pmod 2$, $a \in \mathbb{Z}_q[x]$, $\deg(a) < d$, 则存在惟一的 $b \in \mathbb{Q}_q[x]$ 及 $f \in A^-$, 使得 $\deg(b) < d$ 且

$$\omega = ay^{-m}(dx)/y = b(dx)/y + df,$$

其中 $f = \sum_{j=-m+1}^{-1} f_j y^j$, $f_j \in \mathbb{Q}_q[x]$, $\deg(f_j) < d$. 同时, 对所有的 j 有

$$p^{[\log_p(m-1)]} b \in \mathbb{Z}_q[x], \quad p^{[\log_p(m-1)]} f_j \in \mathbb{Z}_q[x].$$

证明　b 和 f 的存在性可由定理 13.5 证明的最后部分的约化算法直接导出, 故只要证明剩下关于它们分母的界估计.

设 α 是 $Q(x) = 0$ 在某个 $\mathbb{Z}_{q^r}$ 中的一个根, 令 $P = (\alpha, 0)$, 则 y 是 P 点的局部坐标. 于是 $\mathbb{Z}_{q^r}[x, y]/(Q)$ 在 P 处的完备化是 $\mathbb{Z}_{q^r}[[y]]$. 因此, 可以将 df 和 f 表为以下级数:

$$df = \sum_{j \geqslant -m} c_j y^j dy, \quad f = \sum_{j \geqslant -m} \frac{c_j}{j+1} y^{j+1},$$

其中 $c_j \in \mathbb{Q}_{q^r}$, $c_j = 0$(如果 $j \equiv 1 \pmod 2$, 这是因为 $f \in A^-$). $b(dx)/y$ 在 P 处用 y 表达的级数展开式没有极点, 而 $ay^{-m}(dx)/y$ 的级数具有系数在 $\mathbb{Z}_{q^r}$ 中, 因此 $c_j \in \mathbb{Z}_{q^r}$(若 $j < 0$). 令 $n = p^{[\log_p(m-1)]}$, 则 $nc_j/(j+1) \in \mathbb{Z}_{q^r}$(对于 $j < 0$). 计算恒等式 $f = \sum_{j=-m+1}^{-1} f_j y^j$ 的 y^{-m+1} 项的系数, 知 $f_{-m+1}(P) = c_{-m}/(-m+1)$, 故 $nf_{-m+1}(P) \in \mathbb{Z}_{q^r}$. 注意这样的性质在 y 的每一个零点都成立, 因此 $nf_{-m+1} \in \mathbb{Z}_q[x]$(这是因为 $\overline{Q}$ 的 d 个根互不相同, 而 nf_{-m+1} 模 p 后若不为零, 则不会有多于 $d-1$ 个根).

现在 $nf - nf_{-m+1}y^{-m+1}$ 的级数中 y^j $(j < 0)$ 的系数是整的. 同样的证明过程表明 nf_{-m+2} 是整的, ……, 如此这样下去, 则证得引理.

引理 13.2　设 $\omega = ay^m(dx)/y$, $m > 0$, $m \equiv 0 \pmod 2$, $a \in \mathbb{Z}_q[x]$, $\deg(a) < d$, 则存在惟一的 $b \in \mathbb{Q}_q[x]$ 及 $f \in A^-$, 使得 $\deg(b) < d$ 且

$$\omega = ay^m(dx)/y = b(dx)/y + df,$$

其中 $f = \sum_{j=1}^{m-1} f_j y^j$, $f_j \in \mathbb{Q}_q[x]$, $\deg(f_j) < d$. 同时, 还有

$$p^{[\log_p(md+d-2)]} b \in \mathbb{Z}_q[x], \quad p^{[\log_p(dm+d-2)]} f_j \in \mathbb{Z}_q[x], \text{对一切} j.$$

证明　b 和 f 的存在与惟一性由前述约化算法保证. 此时, 我们研究的是 y 的正幂次, 与引理 13.1 的证明类似, 但此时在 y 的 (惟一) 极点 ∞ 处进行研究. 于

是有

$$v_\infty(x) = -2, \quad v_\infty(y) = -d \ (\text{因为} y^2 = Q \text{且} \deg(Q) = d),$$
$$v_\infty(dx) = -3, \quad v_\infty\left(\frac{dx}{y}\right) = d - 3,$$
$$v_\infty(f) \geqslant -md - d + 2,$$
$$v_\infty\big(b(dx)/y\big) \geqslant -d + 1.$$

在 ∞ 点的一个局部坐标可由 $z := x^{\frac{d-1}{2}}/y$ 给出. 注意 $l(z) = -z$, 于是有展开式

$$df = \sum_{j \geqslant -dm-d+1} c_j z^j dz, \quad f = \sum_{j \geqslant -dm-d+1} \frac{c_j}{j+1} z^{j+1},$$

其中 $c_j \in \mathbb{Q}_q$, $c_j = 0$(对 $j \equiv 1 \pmod 2$). 因为 $ay^m(dx)/y$ 的展开式具有系数在 $\mathbb{Z}_q$ 中, 且 $v_\infty\big(b(dx)/y\big) \geqslant -d+1$, 从而导出对 $j \leqslant -d$, 有 $c_j \in \mathbb{Z}_q$. 令 $n = p^{[\log_p(md+d-2)]}$, 则 $nc_j/(j+1) \in \mathbb{Z}_j$(对 $j \leqslant -d$), 因为所有 $v_\infty(x^i y^j)(0 \leqslant i < d, j > 0)$ 都互不相同, 且均不大于 $-d$, 故对所有 j, 有 $nf_j \in \mathbb{Z}_q[x]$, 证毕.

§13.3 Frobenius 提升

在本节中, 我们讨论 Frobenius 自同态 $F_q\colon C'_{\overline{Q}} \to C'_{\overline{Q}}$ 到 $A^\dagger$ 的提升, 以及它在上同调空间 $H^1_{DR}(C'_{\overline{Q}})^-$ 上的作用. 因为上同调空间具有一组清晰的基 $[x^i(dx)/2y]$ $0 \leqslant i < d-1$, 故计算 F_q 在其上的作用等价于计算 F_q 关于这组基的矩阵.

首先看如何将态射 $F_q\colon C'_{\overline{Q}}(\mathbb{F}) \to C'_{\overline{Q}}(\mathbb{F})$($\mathbb{F}$ 是 $\mathbb{F}_q$ 的代数闭包), 描述成一个从 $\mathbb{F}_q$ 代数 $\overline{A}(:= \mathbb{F}_q[x, y, y^{-1}]/(y^2 - \overline{Q}))$ 到 $\overline{A}$ 的一个态射. 态射 F_q 将 $(a, b) \in C_{\overline{Q}}(\mathbb{F})$ 映射到 (a^q, b^q). 由 $\overline{A}$ 的定义, 有

$$C_{\overline{Q}}(\mathbb{F}) = \mathrm{Hom}_{\mathbb{F}_q}(\overline{A}, \mathbb{F}),$$

此处, $(a, b) \in C_{\overline{Q}}(\mathbb{F})$ 对应到如下态射: $\overline{A} \to \mathbb{F}$, $x \mapsto a, y \mapsto b$, 则立即可知映射 $(a, b) \to (a^q, b^q)$ 是由 $\mathbb{F}_q$ 代数态射 $F_q\colon \overline{A} \to \overline{A}$, $x \mapsto x^q$, $y \mapsto y^q$, 诱导出来的. 因为 $q = p^n$, 故 $F_q = F_p^n$, $F_p\colon \overline{A} \to \overline{A}$, $a \mapsto a^p$, $\forall a \in \overline{A}$, 即 F_p 是绝对 p 次 Frobenius 自同态. 从计算的角度来看, 利用 F_p 进行工作是很好的, 但要注意 F_p 并不是一个 $\mathbb{F}_q$-代数态射 (若 $n > 1$). 事实上, 我们有以下交换图表:

$$\begin{array}{ccc} \overline{A} & \xrightarrow{F_p} & \overline{A} \\ \uparrow & & \uparrow \\ \mathbb{F}_q & \xrightarrow[\sigma]{} & \mathbb{F}_q \end{array} \qquad \begin{array}{cccc} \sigma: & \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ & a & \longmapsto & a^p \end{array}$$

此处 σ 是 $\mathbb{F}_q$ 上的绝对 Frobenius.

因为 $\sigma:\ \mathbb{F}_q\to\mathbb{F}_q$ 可以惟一地提升为 $\mathbb{Z}_q$ 的一个自同构, 记之为 σ. 又因为 $\mathbb{Q}_q=\mathbb{Z}_q[1/p]$, σ 可惟一扩充为 $\mathbb{Q}_q$ 的一个自同构. 扩充 σ 到

$$F_p:\ \mathbb{Z}_q[x]\to\mathbb{Z}_q[x],\ x\mapsto x^p.$$

我们将证明 F_p 能惟一扩充到 A^∞ 的一个自同态 F_p, 它是 p-adic 连续的, 且与 A^∞ 上的 $\mathbb{Q}_q[x]$ 代数结构相合, 也就是说, F_p 将子环 A_+^∞(它是 $\mathbb{Z}_q[x,y,z]/(y^2-Q,yz-1)$ 的 p-adic 完备化) 映到自身, 且对每一个 $m\geqslant 0$, 在 $\mathbb{Z}_q[x,y,z]/(y^2-Q,yz-1,p^m)$ 上的 F_p 如果限制到 $\mathbb{Z}_q[x]/(p^m)$ 将是我们已有的 F_p.

令 $Q=x^d+Q_{d-1}x^{d-1}+\cdots+Q_0$, 则有

$$F_pQ=x^{pd}+\sigma(Q_{d-1})x^{p(d-1)}+\sigma(Q_0)=Q^\sigma(x^p).$$

因为 F_p 是 $\mathbb{F}_q[x]$ 上的 p- 次幂 Frobenius 自同态的提升, F_pQ 和 Q^p 在 $\mathbb{F}_q[x]$ 中具有相同的像, 因此它们在 $\mathbb{Z}_q[x]$ 中的差被 p 整除. 令

$$E:=\frac{F_pQ-Q^p}{p}\in\mathbb{Z}_q[x].$$

由构造可知: 扩充 F_p 到 A_+^∞ 意味着

(1) $F_pa=\sigma a,\ \forall a\in\mathbb{Z}_q,$

(2) $F_px=x^p,$

(3) $F_py\in A_+^\infty$ 满足 $(F_py)^2=F_pQ$ 且在 $\overline{A}$ 中的像为 y^p,

(4) $F_pz\in A_+^\infty$ 满足 $(F_py)(F_pz)=1$.

在 A_+^∞ 中, 有

$$F_pQ=Q^p+pE=y^{2p}+pE=y^{2p}(1+pEz^{2p}),$$

故可以令

$$F_py=y^p(1+pEz^{2p})^{1/2}=y^p\sum_{k\geqslant 0}\binom{1/2}{k}p^kE^kz^{2pk},\tag{13.5}$$

此处 $\binom{1/2}{k}$ 是多项式 $\binom{t}{k}=t(t-1)\cdots(t-k+1)/k!$ 在 $t=1/2$ 处的值.

注意 $v(\binom{1/2}{k})\geqslant 0$, 即 $\binom{1/2}{k}\in\mathbb{Z}_q$. 我们也置

$$F_pz=z^p\big(1+pEz^{2p}\big)^{-1/2}=z^p\sum_{k\geqslant 0}\binom{-1/2}{k}p^kE^kz^{2pk},\tag{13.6}$$

于是就将 F_p 扩充到了 A_+^∞, 因此扩充到了 A^∞. 现在设

$$a=\sum_{i,j}a_{ij}x^iy^j\in A^\dagger,\quad 0\leqslant i<d,\ j\in\mathbb{Z},$$

则

$$F_p a = \sum_{i,j} \sigma(a_{ij}) x^{pi} \big(F_p y\big)^j \in A^{\infty},$$

此处对 $j < 0$, 令 $\big(F_p y\big)^j = \big(F_p z\big)^{-j}$. 可以证明 $F_p a \in A^{\dagger}$, 因此, 我们已将 F_p 提升到了 $A^{\dagger}$.

$A^{\dagger}$ 上的 Frobenius 提升 F_p 在 $A^{\dagger}$ 的 de Rham 复形上诱导出一个 σ 线性映射, 从而诱导出 $\mathbb{Q}_q$ 向量空间 $H^1(C_{\overline{Q}})^-$ 上的一个 σ 线性映射. 回忆到 $[x^i(dx)/y](0 \leqslant i < d-1)$ 形成该上同调空间的一组基, 有

$$F_p: \; x^i(dx)/y \mapsto px^{pi+p-1} y \big(F_p y\big)^{-1}(dx)/y = px^{p(i+1)-1} y \big(F_p z\big)(dx)/y,$$

而

$$y(F_p z) = y^{-p+1} \sum_{k \geqslant 0} \binom{-1/2}{k} p^k E^k y^{-2pk},$$

因此

$$F_p\big(x^i(dx)/y\big) = \sum_{k \geqslant 0} \binom{-1/2}{k} p^{k+1} E^k x^{p(i+1)-1} y^{-(2k+1)p+1} \cdot (dx)/y.$$

E 的次数最多为 $pd-1$, 故 $E^k x^{p(i+1)-1}$ 最多为 $p(d-1)-1+k(pd-1)$ 次. 但

$$\frac{k(pd-1)+p(d-1)-1}{d} < (k+1)p,$$

故对于 $k \geqslant 0$, 有

$$\begin{aligned} &\binom{-1/2}{k} E^k x^{p(i+1)-1} y^{-(2k+1)p+1} \\ = &\sum_{-(2k+1)p<j<p} c_{i,k,j} y^j, \quad c_{i,k,j} \in \mathbb{Z}_q[x], \deg(c_{i,k,j}) < d. \end{aligned}$$

从而, 对 $0 \leqslant i < d-1$, 有

$$F_p(x^i(dx)/y) = \sum_{\substack{k \geqslant 0 \\ -(2k+1)p<j<p}} p^{k+1} c_{i,k,j} y^j \cdot (dx)/y.$$

应用引理 13.1 和 13.2, 有

$$[F_p(x^i(dx)/y)] = \Big[\sum_{k \geqslant 0} p^{k+1} c'_{i,k}(dx)/y\Big],$$

此处 $[*]$ 表示 $*$ 所在上同调类, 而 $c'_{i,k} \in \mathbb{Q}_q[x]$, $\deg(c'_{i,k}) < d$, $p^{m_k} c'_{i,k} \in \mathbb{Z}_q[x]$, $m_k = \max\left([\log_p((2k+1)p)], [\log_p(pd-2)]\right)$. 但是 $F_p(x^i(dx)/y)$ 还未完全约化, 因为 $x^{d-1}(dx)/y$ 还有可能出现在上式右端. 最后的约化步骤需要运用微分 dy 和关于整数 d 的一个除法. 若 $p \nmid d$, 这个除法将给出一个整数 ($\mathbb{Z}_q$ 中), 从而 Frobenius 在 $H^1(C'_{\overline{Q}})^-$ 上的作用由 $\mathbb{Z}_q$ 上的一个矩阵给出. 但一般而言, p 有可能整除 d, 故需要另行考虑如下: 设 $c''_{i,k} \in \mathbb{Q}_q[x]$, 使得 $\deg(c''_{i,k}) < d-1$ 且 $[c'_{i,k}(dx)/y] = [c''_{i,j}(dx)/y]$, 则

$$[F_p(x^i(dx)/y)] = \Big[\sum_{k\geqslant 0} p^{k+1} c''_{i,k}(dx)/y\Big],$$

其中 $c''_{i,k} \in \mathbb{Q}_q[x]$, $\deg(c''_{i,k}) < d-1$, $p^{m_k+v_p(d)} c''_{i,k} \in \mathbb{Z}_q[x]$.

因为我们考虑 F_p 的 n 次幂在 $H^1(C'_{\overline{Q}})^-$ 上的作用, 故自然希望知道是否 $\mathbb{Z}_q$ 模

$$\bigoplus_{0\leqslant i<d-1} \mathbb{Z}_q \cdot x^i(dx)/y$$

在 F_p 作用下是稳定的, 即 F_p 关于这组基的矩阵是否在 $\mathbb{Z}_q$ 中. 事实上, 上面的计算表明

$$\min\{k+1-m_k-v_p(d) \mid k \geqslant 0\} = -v_p(d) - [\log_p(d-2/p)]$$

可以取负值, 从而该矩阵有可能不在 $\mathbb{Z}_q$ 中. 下面的引理表明尽管如此, 当计算 F_p^n 的作用时, 该矩阵中元素的分母的赋值不会太大.

引理 13.3　*设 t 是 ∞ 点的局部参数, 使得 $lt = -t$(例如可取 $t := x^g/y$), 令 L 是 $\bigoplus_{0\leqslant i<d-1} \mathbb{Z}_q \cdot x^i(dx)/y$ 的如下元素组成的 $\mathbb{Z}_q$ 子模: $\omega \in L$ 当且仅当 ω 在 $(t^{-2g}\mathbb{Z}_q[[t]]dt)/(t^{-1}\mathbb{Z}_q[[t]]dt)$ 中的像能够积分, 也即, 是在下面的像中:*

$$d:\ \frac{t^{-2g+1}\mathbb{Z}_q[[t]]}{\mathbb{Z}_q[[t]]} \longrightarrow \frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt},$$

则 F_p 在 $H^1(C'_{\overline{Q}})^-$ 上的作用保持 $\mathbb{Z}_q$ 模 L, 且有一个同构

$$\frac{\bigoplus_{0\leqslant i<d-1} \mathbb{Z}_q \cdot x^i(dx)/y}{L} \simeq \bigoplus_{\substack{-(2g-1)\leqslant i<0 \\ i\equiv 1 \pmod 2}} \mathbb{Z}_q/i\mathbb{Z}_q,$$

因此, 商 $\bigoplus_{0\leqslant i<d-1}(\mathbb{Z}_q \cdot x^i(dx)/y)/L$ 被 $p^{[\log_p(2g-1)]}$ 零化.

证明省略.

设 $e = (e_1, \cdots, e_{2g})$ 是 L 的一组 $\mathbb{Z}_q$ 基, 令 m 是 F_p 在 L 上关于 e 的矩阵, 于是

$$F_p e_j = \sum_i m_{ij} e_i.$$

于是引理 13.3 表明 $m \in M_{2g}(\mathbb{Z}_q)$. 因为 F_p 是 σ 线性的, 故有

$$F_p\Big(\sum_j \lambda_j e_j\Big) = \sum_{i,j} \sigma(\lambda_j) m_{ij} e_i, \quad \forall \lambda_j \in \mathbb{Z}_q.$$

另一方面 $F_q = F_p^n$, 故 F_q 在 $H^1(C'_{\overline{Q}})^-$ 上关于基 e 的矩阵就是

$$\big(\mathrm{mat}(F_q)\big)_e = m \cdot (m^{\sigma}) \cdots (m^{\sigma^{n-1}}).$$

这是因为以下事实: 若 a 和 b 是 $\mathbb{Q}_q$ 向量空间 V 上的 σ 线性自同态, 则有

$$\mathrm{mat}(ab)_e = (\mathrm{mat}(a)_e)\big(\mathrm{mat}(b)_e\big)^{\sigma},$$

其中 e 是 V 的一组基, $\mathrm{mat}(*)_e$ 表示 $*$ 关于基 e 的矩阵.

结合定理 13.3 和 13.4 及上面的讨论, 有

定理 13.7 F_p^n 在 $\mathbb{Q}_q$ 向量空间 $H^1(C'_{\overline{Q}})^-$ 上的特征多项式是

$$P_{\overline{Q}} = \prod_{i=1}^{2g}(t-\alpha_i) = t^{2g} - a_1 t^{2g-1} + \cdots - a_{2g-1}t + a_{2g}.$$

我们有: $a_{2g-i} = q^{g-i}a_i$, $|a_i| \leqslant 2^{2g}q^{i/2}$.

证明 由定理 13.4 知 F_p^n 的特征多项式是 $P_{\overline{Q}}$, 由定理 13.3 知 $\alpha_i\alpha_{g+i} = q$, 由此推出 $a_{2g-i} = q^{g-i}a_i$, 最后, 由 $|\alpha_i| = q^{1/2}$, 知

$$|a_i| = \Big|\sum_{j_1<\cdots<j_i} \alpha_{j_1}\cdots\alpha_{j_i}\Big| \leqslant \sum |\alpha_{j_1}\cdots\alpha_{g_i}| = \binom{2g}{i} q^{i/2} \leqslant 2^{2g}q^{i/2}.$$

这就完成了证明.

注记 13.1 由定理 13.7 知, 为了计算 a_i(作为 $\mathbb{Z}_q/p^N\mathbb{Z}_q$ 中元素), $1 \leqslant i \leqslant g$, 只要取 N 使得 $p^N > 2 \cdot 2^{2g} \cdot q^{g/2}$ 即可.

§13.4 算法综述

在本节中, 我们将前 3 节的理论讨论具体描述成可实现的算法.

(算法 13.2) Kedlaya 算法

输入: 有限域 $\mathbb{F}_q$ ($q = p^n$, $p > 2$, $\mathbb{F}_p[z]$ 中的一个 n 次首一不可约多项式 $\overline{f}$, (从而 $\mathbb{F}_q = \mathbb{F}_p[z]/(f)$)), $d = 2g+1 \geqslant 1$, $\mathbb{F}_q[x]$ 中一个 d 次首一不可约多项式 $\overline{Q}$, 使得 $(\overline{Q}, \overline{Q}') = 1$.

输出：定理 13.7(也就是定理 13.3) 中的多项式 $P_{\overline{Q}}$.

预计算：

1. 提升 $\overline{f}$ 到 $f \in \mathbb{Z}[z]$, f 的系数 $\in \{0,1,\cdots,p-1\}$, 令 $\mathbb{Z}_q := \mathbb{Z}_p[z]/(f)$.

2. 提升 $\overline{Q}$ 到 $Q \in \mathbb{Z}_q[x]$: $Q = x^d + Q_{d-1}x^{d-1} + \cdots + Q_0$, 其中 $Q_i = \sum_{0 \leqslant j < n} Q_{ij}z^j \in \mathbb{Z}_q = \mathbb{Z}_p 1 \oplus \cdots \oplus \mathbb{Z}_p z^{n-1}$, $Q_{ij} \in \{0,1,\cdots,p-1\}$.

3. 令 $N := \lceil \log_p(2^{2g+1}q^{g/2}) \rceil$ (故 $p^N > 2^{2g+1}q^{g/2}$),
$N_1 := N + v_p(d) + \lfloor \log_p(d-2/p) \rfloor + \lfloor \log_p(2g-1) \rfloor$.

4. 令 M 是满足下式的最小正整数：

$$M - \lfloor \log_p(2M+1) \rfloor \geqslant N_1.$$

第 1 步：令 p-adic 运算精度为 N_1, 而对于级数计算的最大精度为 M.

第 2 步：令 $S = 1 + \left(Q(x)^\sigma - Q(x)^p\right)\tau^p$, $Q(x)$ 的系数属于 $\mathbb{Z}_q$, 精度到 p^{N_1}.

第 3 步：计算 $S^{-1/2}$ 作为 τ 的级数, 到精度 τ^M. 这可以用牛顿迭代 $X \longleftarrow \frac{1}{2}(3X - SX^3)$, 初始条件为 $X=1$. 而在每一步迭代过程中, 用第 2 节中的 Reduction Step 1 保持级数的系数次数不大于 $d-1$.

第 4 步：计算

$$\begin{aligned}\omega = \left(\frac{x^i dx}{y}\right)^\sigma &= \frac{px^{p(i+1)-1}dx}{y^\sigma} \\ &= \left(y^{-1}\tau^{\frac{p-1}{2}} \sum_{k \geqslant 0} P_k(x)\tau^{pk}\right) px^{p(i+1)-1}dx \\ &= \left(\sum_{k \geqslant 0} Q_k(x)\tau^k\right)\frac{dx}{y}\end{aligned}$$

作为 τ 的级数, 到精度 τ^M.

第 5 步：应用第 2 节中的 Reduction Step 2, 将 ω 写成 $Q(x)\frac{dx}{y}$ 的形式.

第 6 步：应用第 2 节中的 Reduction Step 3, 将 $Q(x)$ 的次数降到不大于 $2g-1$.

第 7 步：形成矩阵 M, 使得

$$\begin{pmatrix} \frac{dx}{y} \\ \frac{xdx}{y} \\ \vdots \\ \frac{x^{2g-1}dx}{y} \end{pmatrix}^\sigma = M \begin{pmatrix} \frac{dx}{y} \\ \frac{xdx}{y} \\ \vdots \\ \frac{x^{2g-1}dx}{y} \end{pmatrix}.$$

第 8 步：计算矩阵

$$F := M \cdot M^\sigma \cdot M^{\sigma^2} \cdots M^{\sigma^{n-1}}.$$

第 9 步: 计算矩阵 F 的特征多项式, 设它为 P.

第 10 步: 输出 $P_{\overline{Q}} := P$.

最后, 我们分析研究计算复杂度, 设 p 是一个固定的小素数. 首先, 算法中所有环运算都是在 $\mathbb{Z}_p/(p^{N_1})$ 的一个 n 次非分歧扩张中进行, 该环中每个元素需要 $O(gn^2)$ 的存储空间. 应用快速整数乘法, 环中每个乘法和除法可在 $O(g^{1+\varepsilon}n^{2+\varepsilon})$ 时间内完成.

其次, 环自同构 σ 的任何一个幂次 σ^k 可在 $O(g^{1+\varepsilon}n^{3+\varepsilon})$ 时间内完成. 设基环表示为 $\mathbb{Z}_p/(p^{N_1})[\alpha]$, 此处 $P(\alpha)=0$. 通过重复平方算法, 计算出剩余类域中一个元素, 它模 p 同余 α^{p^k}. 然后应用牛顿迭代由此计算 α^{σ^k}, 而后可计算任何 $G(\alpha)^{\tau}$, G 为 $\mathbb{Z}_p/(p^N)$ 中多项式 (借助 Paterson-Stockmeyer 算法), 这需要 $O(n)$ 个 $\mathbb{Z}_p/(p^N)$ 中乘法.

在第 3 步中, 计算 $1/y^{\sigma}$ 的 $O(gn)$ 个项, 每项由一个次数不超过 $2g-1$ 的 x 的多项式组成. 它需要 $O(g^2n^2)$ 存储空间, 故全部需要空间 $O(g^3n^3)$, 时间 $O(g^{3+\varepsilon}n^{3+\varepsilon})$.

在第 4~6 步中, 这是主要计算步骤, 每一个约化是将一个次数不超过 $2g-1$ 的多项式 T 写成 $AQ+BQ'$ 的形式. 这可以通过预运算计算次数 $2g-1$ 和 $2g$ 的多项式 R 和 S, 使得 $RQ+SQ'=1$ 来完成. 然后计算 A 作为 TQ 模 Q', 而 B 是 SQ' 模 Q. 因为在问题中的多项式每个要求 $O(g^{2+\varepsilon}n^{2+\varepsilon})$ 存储空间, 这个扩充的 GCD 运算能够在 $O(g^{2+\varepsilon}n^{2+\varepsilon})$ 时间内完成. 约化步骤对 $2g$ 个微分进行. 每一个微分需要 $O(gn)$ 个约化步骤, 故共耗时 $O(g^{4+\varepsilon}n^{3+\varepsilon})$. 在第 8 和 9 步中, 我们始于矩阵 $M\in M_{2g}(\mathbb{Z}_q)$, 其每一个元素具有尺度 $O(gn^2)$, 且需用重复平方法计算 $F=M\cdot M^{\sigma}\cdot M^{\sigma^2}\cdots M^{\sigma^{n-1}}$, 即计算

$$M_1=MM^{\sigma}, M_2=M_1M_1^{\sigma^2}, M_3=M_2M_2^{\sigma^4}, \cdots,$$

然后结合通常的指数幂运算的重复平方算法以计算 F. 这个过程需要 $O(\log n)$ 个 $2g\times 2g$ 矩阵的乘法, 以及 $O(g^2\log n)$ 个 σ 的幂次的应用 (特别地, σ^m, m 是 2 的幂次). 前者要 $O(g^3\log n)$ 个环运算, 耗时 $O(g^{4+\varepsilon}n^{2+\varepsilon})$, 后者耗时 $O(g^{3+\varepsilon}n^{3+\varepsilon})$. 第 9 步可以在 $O(g^3)$ 个环运算中完成. 因此, 总共需要存储空间 $O(g^3n^3)$, 耗时 $O(g^{4+\varepsilon}n^{3+\varepsilon})$.

§13.5 推广到 Superelliptic 曲线

在本节中, 我们将前面的讨论推广到一类包含超椭圆曲线 (hyperelliptic curves) 作为特例的所谓 Superellipeic 的曲线上.

仍设 p 是一素数, $q=p^n$.

定义 13.2 称平面曲线 C 是一条superelliptic曲线, 如果它可以由平面仿射

方程

$$y^r = f(x)$$

定义, 其中 r 是一个不等于 p 的素数, 而 f 是首一的次数为 d 的无平方因子多项式, 且 $(d,r)=1$.

该曲线的亏格 $g=\frac{(d-1)(r-1)}{2}$. 特别地, 如果 $r=2$, 则 superelliptic 曲线就是前面讨论的超椭圆曲线.

因为 Weil 猜想对一般的代数簇均成立, 所以我们知道定理 13.3 对 superelliptic 曲线同样成立. 于是, 若设 C 是亏格 g 的 superelliptic 曲线, 记 F_q 是其上的 q 次 Frobenius 自同态, 则其特征多项式 $P_f(T)$ 具有以下形式:

$$P_f(T)=\sum_{i=0}^{2g} a_i T^i, \quad a_0=a_{2g}=1, \quad a_{2g-i}=q^i a_i, \quad i=1,2,\cdots,g-1,$$

$P_f(T)$ 的所有根均具有绝对值 $\sqrt{q}$, 且 C 的 Jacobian 簇 $J(C)$ 在 $\mathbb{F}_q$ 上的有理点的数目 $\#J(C)=P_f(1)$. 本节的目的就是给出计算 $P_f(T)$ 的一个算法, 从而可以知道 $\#J(C)$.

假定所有的记号都与前面 4 节中相同, 特别地, $\mathbb{Q}_q$ 记 $\mathbb{Q}_p$ 的 n 次非分歧扩张, $\mathbb{Z}_q$ 是 $\mathbb{Q}_q$ 的赋值环. 它具体构造如下: 取一个首一不可约多项式 $\overline{P}(t)\in\mathbb{F}_p[t]$, 则 $\mathbb{F}_q=\mathbb{F}_p[t]/(\overline{P}(t))$. 平凡地提升 $\overline{P}(t)$ 到 $P(t)\in\mathbb{Z}_p[t]$, 则 $\mathbb{Z}_q:=\mathbb{Z}_p[t]/(P(t))$. 特别地, $z\in\mathbb{Z}_q$ 能表示为 $z_{n-1}t^{n-2}+\cdots z_1 t+z_0$, $z_i\in\mathbb{Z}_p$. 记 σ 是 $\mathbb{Q}_q$ 上的 p 次 Frobenius 自同构. 它是 $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ 的生成元, σ 是 $\mathbb{F}_q$ 上的 p 次 Frobenius 的一个提升. 事实上, 对于 $z\in\mathbb{Z}_q$, 若 $z=\sum_{i=0}^{n-1} z_i t^i$, 则

$$z^\sigma=\Big(\sum_{i=0}^{n-1} z_i t^i\Big)^\sigma=\sum_{i=0}^{n-1} z_i (t^i)^\sigma,$$

因此, 只要能预先计算出 t^σ, 则任何元素 $z\in\mathbb{Z}_q$ 在 σ 下的像就可利用上式算出.

现在设 C 是由方程

$$y^r=\overline{f}(x), \qquad \deg(f)=d$$

给出的 superelliptic 曲线, 则前几节关于超椭圆曲线的理论可完全类似地推广到现在的情形. 特别地, 我们有

定理 13.8 上同调类元素 $[\frac{x^i dx}{y^j}](0\leqslant i<d-1, 1\leqslant j\leqslant r-1)$, 形成 $H^1(C'_{\overline{f}})^-$ 的一组基, 而 F_q^* 在 $H^1(C'_{\overline{f}})^-$ 上特征多项式就是 $P_{\overline{f}}(T)$.

类似地, C 上的 p 次 Frobenius 的提升 σ 的作用可如下定义: $x^\sigma=x^p$, $(y^\sigma)^r=(f(x))^\sigma$, $(dx)^\sigma=px^{p-1}dx$. 而微分形式的空间在 σ 的作用下是稳定的. 下面描述类

似的 Reduction 过程, 它将 $(\frac{x^i dx}{y^j})^\sigma$ 仍约化到定理 13.8 中那组基. 固定 $0 \leqslant i < d-1$, $1 \leqslant j \leqslant r-1$, 写 $(\frac{1}{y^j})^\sigma$ 成一个幂级数

$$\left(\frac{1}{y^j}\right)^\sigma = y^{-jp}\left(1 + \frac{f(x)^\sigma - f(x)^p}{y^{rp}}\right)^{-j/r} = y^{-jp}\sum_{k\geqslant 0} P_k(x)\tau^{pk},$$

其中 $\tau = y^{-r}$, 故有

$$\left(\frac{x^i dx}{y^j}\right)^\sigma = \left(\sum_{k\geqslant 0} Q_k(x)\tau^k\right)\frac{dx}{y^{jp \pmod r}},$$

其中 $Q_k(x)$ 是一些多项式. 下面记 $l = jp \pmod r$, 于是有以下类似的约化算法:

(算法 13.3) Reduction 算法

Step 1: 首先, 利用曲线的方程, 做以下带余除法:

$$Q_k(x) = \alpha_k(x)f(x) + \beta_k(x), \qquad \deg(\beta_k) < \deg(f) = d.$$

于是

$$Q_k(x)\tau^k = \big(\alpha_k(x)f(x) + \beta_k(x)\big)\tau^k = \alpha_k(x)\tau^{k-1} + \beta_k(x)\tau^k.$$

故可以将 $Q_k(x)$ 仍约化到次数最多为 $d-1$(除了 $Q_0(x)$ 外);

Step 2: 其次, 降低 τ^k 的次数 k: 对 $k \geqslant 1$, 令 $u(x)$ 和 $v(x)$ 是多项式, 使得 $Q_k(x) = u(x)f(x) + v(x)f'(x)$, 则有

$$Q_k(x)\tau^k\frac{dx}{y^l} \equiv \left(u(x) + \frac{r}{r(k-1)+l}v'(x)\right)\tau^{k-1}\frac{dx}{y^l}.$$

Step 3: 最后, 剩下表达式 $Q(x)\frac{dx}{y^l}$, 其中 $Q(x)$ 是次数为 δ 的多项式. 若 $\delta \geqslant d-1$, 则正合微分 $d\big(x^{\delta-(d-1)}y^{r-l}\big) \equiv 0$ 给出一个次数 δ 的多项式, 于是 $Q(x)$ 减去 $d\big(x^{\delta-(d-1)}y^{r-l}\big)$ 的适当倍数就可将 $Q(x)\frac{dx}{y^l}$ 的次数降下去.

由以上 Reduction 算法, 就可以计算出一个 $2g\times 2g$ 矩阵 $M \in M_{2g}(\mathbb{Z}_q)$,

$$\left(\frac{x^i dx}{y^j}\right)^\sigma_{ij} = M\left(\frac{x^i dx}{y^j}\right)_{ij},$$

于是与超椭圆曲线情形类似, 可以算出 $F_q = \sigma^n$ 的矩阵为

$$F = M\cdot M^\sigma \cdots M^{\sigma^{n-1}}.$$

再计算 F 的特征多项式即可得到所求多项式 $P_f(T)$. 下面给出具体的算法:

(算法 13.4) 对于 Superelliptic 曲线的 Kedlaya 算法

输入: $\mathbb{F}_q$ 上一条 superelliptic 曲线: $y^r = \overline{f}(x)(q=p^n,\ d=\deg(\overline{f}))$.

输出: 多项式 $P_f(T)$.

Step 1: 令 $v := \lceil \log_p(2\binom{2g}{g}q^{g/2})\rceil$, μ 是满足 $\mu > pv + p\log_p\big((r+1)\mu - 1\big)$ 的最小正整数.

Step 2: 令 $S = 1 + \big(f(x)^\sigma - f(x)^p\big)\tau^p$, 其中 $f(x)$ 是 $\overline{f}(x)$ 在 $\mathbb{Z}_q[x]$ 中的平凡提升.

Step 3: 计算 $S^{-1/r}$ 作为 τ 的级数, 精度到 τ^μ(这可以用牛顿迭代来完成: $X \longleftarrow \frac{1}{r}\big((r+1)X - SX^{r+1}\big)$, 初始条件 $X=1$, 在每一步递归中, 用 Reduction 算法中的 Step 1 保持级数的系数的次数不超过 $d-1$).

Step 4: 计算 $S^{-j/r}$ 到精度 τ^μ, 其中 $2 \leqslant j \leqslant r-1$, 这可以由 $S^{-1/r}$ 不断自乘得出, 当然在每次相乘后要用 Reduction 算法中的 Step 1 进行约化, 以使系数的次数不超过 $d-1$.

Step 5: 对每一个 $i, j(0 \leqslant i < d-1,\ 1 \leqslant j \leqslant r-1)$ 计算

5.1 计算 $\omega_{ij} = (\frac{x^i dx}{y^j})^\sigma = p\tau^{jp\,\mathrm{div}\,r}x^{ip+p-1}S^{-j/r}\frac{dx}{y^{jp \bmod r}}$, 其中 $jp\,\mathrm{div}\,r$ 和 $jp \bmod r$ 分别表示 jp 被 r 除所得的商和余数.

5.2 应用 Reduction 算法中的 Step 2, 将 ω_{ij} 写成形式 $Q(x)\frac{dx}{y^{jp \bmod r}}$.

5.3 应用 Reduction 算法中的 Step 3, 将 $Q(x)$ 的次数降到 $d-1$ 以下.

Step 6: 形成矩阵 M, 使得

$$\left(\frac{x^i dx}{y^j}\right)^\sigma_{ij} = M\left(\frac{x^i dx}{y^j}\right)_{ij},$$

计算 M 的范: $F = M \cdot M^\sigma \cdots M^{\sigma^{n-1}}$.

Step 7: 计算 F 的特征多项式: $\widetilde{\chi}(T) = \sum_{0\leqslant i\leqslant 2g}\widetilde{a}_k T^k$.

Step 8: 对 $1 \leqslant k \leqslant g$, 找出整数 $a_k \in [-p^{v-1}, p^{v-1}]$, 使得 $a_k \equiv \widetilde{a}_k \pmod{p^v}$.

Step 9: 令 $a_{2g-i} = q^i a_i,\ 1 \leqslant i \leqslant g-1,\ a_0 = a_{2g} = 1$.

Step 10: 输出多项式 $P_{\overline{f}} = \sum_{i=0}^{2g} a_i T^i$.

我们假定 p 是一个固定的小素数, 同时假设 r 和 d 固定, 下面分析算法的复杂度:

在 Step 2 中, 要计算 $f(x)^\sigma$, 这归结到 t^σ 的计算. 注意 t 是 $P(t)$ 的一个根, 从而 t^σ 亦然. 故 t^σ 能够由牛顿迭代 $X \longleftarrow X - P(X)/P'(X)$ 得到, 初始值取 t^p 可在算法之前通过预运算求得, 因此, $\mathbb{Z}_q$ 中一个元素的 Frobenius 像可在 $O(n^{3+\varepsilon})$ 时间中求得.

Step 3 是牛顿迭代, 所需耗时是最后一次迭代耗时的常数倍. 而最后一次迭代所需是几个计算对应的乘法, 这些计算对应是一些系数在 $\mathbb{Z}_q$ 中的次数 $d-1$ 的多项式的次数为 μ 的多项式, $\mathbb{Z}_q$ 中一个元素的比特尺度为 nv, 这些计算对应的比特尺度为 $nv\mu d = O(n^{3+\varepsilon})$, 故在最后一次迭代中要做的 $O(1)$ 个乘法耗时为 $O(n^{3+\varepsilon})$, 而应用 Reduction 算法中 Step 1 所得结果具有大致相同的复杂度, 因此 Step 3 的复杂度为 $O(n^{3+\varepsilon})$.

在 Step 4 中所需复杂度主要是 Reduction 算法中 Step 1 的约化 (因为 r 假定是常数), 它的复杂度为 $O(n^{3+\varepsilon})$.

在 Step 5 中, 我们要做 $2g$ 次 Reduction 算法中的 Step 2 和 Step 3, 其中 5.1 只是重新组织和 Reduction 算法中 Step 1 的约化, 它的耗时可忽略不计, 而 5.2 重复了 μ 次如下过程: 每次都是 $\mathbb{Z}_q$ 上次数不超过 d 的一些多项式的初等运算, 从而 5.2 耗时 $O(n^{3+\varepsilon})$, 5.3 中的约化过程可忽略不计, 故 Step 5 需时 $O(n^{3+\varepsilon})$.

在 Step 6 中耗时: 通过常用的递归方法计算范数, 需时 $O(n^{3+\varepsilon})$, 其余步骤耗时可忽略不计, 故总耗时数为 $O(n^{3+\varepsilon})$.

在第十三章的最后加上一个注如下:

注记: 本章的主要内容的写作参考了以下文献: K.S.Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer Cohomology. J. of Ramanu jan Math. Soc., 16:323-338, 2001.

第十四章　$\mathbb{F}_{2^n}$ 上超椭圆曲线的 Kedlaya 算法

§14.1　$\mathbb{F}_{2^n}$ 上超椭圆曲线的上同调

设 $\mathbb{F}_q$ 是有限域, $q=2^n$, $\overline{\mathbb{F}}_q$ 是其代数闭包. 考虑由下式定义的亏格 g 的光滑仿射超椭圆曲线 $\overline{C}$:

$$\overline{C}:\quad y^2+\overline{h}(x)y=\overline{f}(x),$$

其中 $\overline{h},\overline{f}\in\mathbb{F}_q[x]$, $\overline{f}$ 是 $2g+1$ 次的首一多项式, $\deg(\overline{h})\leqslant g$. 令

$$\overline{h}(x)=\overline{c}\prod_{i=0}^{s}(x-\overline{\theta}_i)^{m_i},\qquad \overline{\theta}_i\in\overline{\mathbb{F}}_q,\overline{c}\in\mathbb{F}_q^*,$$

定义

$$\overline{H}(x)=\prod_{i=0}^{s}(x-\overline{\theta}_i)\in\mathbb{F}_q[x].$$

若 $\overline{h}(x)$ 为常数, 则定义 $\overline{H}(x)=1$. 不失一般性, 总可以假设 $\overline{H}(x)|\overline{f}(x)$. 事实上, 由下式定义的:

$$x\mapsto x,\qquad y\mapsto y+\sum_{i=0}^{s}\overline{b}_ix^i$$

同构, 将曲线 $\overline{C}$ 变为

$$y^2+\overline{h}(x)y=\overline{f}(x)-\sum_{i=0}^{s}\overline{b}_i^2x^{2i}-\overline{h}(x)\sum_{i=0}^{s}\overline{b}_ix^i.$$

易知 $\overline{H}(x)$ 整除上式右端当且仅当

$$\overline{f}(\overline{\theta}_j)=\sum_{i=0}^{s}\overline{b}_i^2\overline{\theta}_j^{2i},\qquad j=0,1,\cdots,s.$$

这是一个关于 $\overline{b_i}^2$ 的线性方程组, 其系数行列式为 $\{\theta_j^2\}_{j=0}^{s}$ 的 Vandermonde 行列式, 因为 $\overline{\theta_j}$ 是 $\mathbb{F}_q$ 上一个多项式的零点, 故上述方程组在 q 次 Frobenius 作用下是不变的, 从而 $\overline{b_i}^2$(故而 $\overline{b_i}$) 是 $\mathbb{F}_q$ 的元素. 于是我们总可以假定 $\overline{H}(x)|\overline{f}(x)$.

现在记 $\pi:\ \overline{C}(\overline{\mathbb{F}}_q)\to\mathbb{A}^1(\overline{\mathbb{F}}_q)$ 是到 x 轴的投影. 令 $\overline{C}'$ 是从 $\overline{C}$ 上去掉点 $(\overline{\theta}_i,0)(0\leqslant i\leqslant s)$ 后的曲线, 于是 $\overline{C}'$ 的坐标环为

$$\mathbb{F}_q[x,y,\overline{H}(x)^{-1}]/(y^2+\overline{h}(x)y-\overline{f}(x)).$$

令 $\mathbb{Q}_q$ 是 $\mathbb{Q}_2$ 的 n 次非分歧扩张, 其赋值环为 $\mathbb{Z}_q$, 剩余类域为 $\mathbb{F}_q$. 令 $\overline{h}(x) = \overline{c} \cdot \prod_{i=0}^{r} \overline{P}_i(x)^{t_i}$, $\overline{P}_i(x)$ 是 $\mathbb{F}_q$ 上首一不可约多项式. 令 $D = \max_{0 \leqslant i \leqslant r}\{t_i\}$, 则 $\overline{h}(x)|\overline{H}(x)^D$(因 $\overline{H}(x) = \prod_{i=0}^{r} \overline{P}_i(x)$). 提升 $\overline{P}_i(x)(0 \leqslant i \leqslant r)$ 到 $\mathbb{Z}_q[x]$ 上的首一多项式 $P_i(x)$, 令

$$H(x) = \prod_{i=0}^{r} P_i(x), \qquad h(x) = c\prod_{i=0}^{r} P_i(x)^{t_i},$$

c 是 $\overline{c}$ 在 $\mathbb{Z}_q$ 中的任意提升. 因 $\overline{H}(x)|\overline{f}(x)$, 定义 $\overline{Q_{\overline{f}}}(x) = \overline{f}(x)/\overline{H}(x)$. 令 $Q_f(x) \in \mathbb{Z}_q[x]$ 是 $\overline{Q_{\overline{f}}}(x)$ 的任意一个首一提升. 置 $f(x) = H(x)Q_f(x)$, 于是得到 $\overline{\mathcal{C}}$ 在 $\mathbb{Z}_q$ 上的一条提升曲线

$$\mathcal{C}: \quad y^2 + h(x)y = f(x).$$

由上面 $H(x)$ 和 $h(x)$ 及 $f(x)$ 的构造, 有 $H(x)|h(x)$ 和 $H(x)|f(x)$ 及 $h(x)|H(x)^D$. 令 $\mathbb{Q}_q^{ur}$ 是 $\mathbb{Q}_q$ 的极大非分歧扩张, $\mathbb{Z}_q^{ur}$ 是其赋值环. 令 $\theta_k(0 \leqslant k \leqslant s)$ 是 $H(x)$ 的零点, 则 θ_k 是 $\mathbb{Z}_q^{ur}$ 中的单位元. 令

$$\pi: \mathcal{C}(\overline{\mathbb{Q}}_q) \to \mathbb{A}^1(\overline{\mathbb{Q}}_q)$$

是到 x 轴的投影, 则 $(\theta_k, 0)$ 是 π 的分歧点.

考虑曲线 $\mathcal{C}' = \mathcal{C} \setminus \{(\theta_k, 0), 0 \leqslant i \leqslant s\}$, 则 $\mathcal{C}'$ 的坐标环为

$$A = \mathbb{Z}_q[x, y, H(x)^{-1}]/(y^2 + h(x)y - f(x)).$$

易知

$$l: \quad x \mapsto x,\ y \mapsto -y - h(x)$$

是 A 上的一个对合.

令 $A^\dagger$ 是 A 的弱完备化, 其定义如第一章所述. 应用曲线的方程, 则 $A^\dagger$ 中任何元素都可表为下述形式的级数:

$$\sum_{i=-\infty}^{\infty} \big(U_i(x) + V_i(x)y\big)S(x)^i,$$

其中, $\deg\big(U_i(x)\big) < \deg\big(S(x)\big)$, $\deg\big(V_i(x)\big) < \deg\big(S(x)\big)$,

$$S(x) = \begin{cases} H(x), & \text{若 } \deg(H) > 0; \\ x, & \text{若 } H(x) = 1. \end{cases}$$

且存在正数 δ 和 $\varepsilon > 0$, 使得

$$\operatorname{ord}_2\big(U_i(x)\big) \geqslant \varepsilon|i| + \delta, \quad \operatorname{ord}_2\big(V_i(x)\big) \geqslant \varepsilon|i+1| + \delta,$$

其中 $\mathrm{ord}_2\big(P(x)\big)$ 是多项式 $P(x)$ 的系数之 2-adic 赋值之最小者, 即

$$\mathrm{ord}_2\big(P(x)\big) = \min_j\{\mathrm{ord}_2(P_j)\}, \quad P(x) = \sum_j P_j x^j \in \mathbb{Q}_q[x].$$

将 $\mathbb{F}_q$ 上的 2 次 Frobenius 映射 σ 提升到 $\mathbb{Z}_q$ 上, 记为 Σ. 扩充 Σ 到 $A^\dagger$ 上的一个自然同态: $x \mapsto x^2$, $y \mapsto \Sigma(y)$, 满足

$$\Sigma(y)^2 + \Sigma\big(h(x)\big)\Sigma(y) - \Sigma\big(f(x)\big) = 0 \quad 且 \quad \Sigma(y) \equiv y^2 \pmod 2.$$

应用牛顿迭代可以计算出上面方程的解, 它是 A 的 2-adic 完备化中的元素:

$$W_{k+1} \equiv W_k - \frac{W_k^2 + \Sigma\big(h(x)\big)W_k - \Sigma\big(f(x)\big)}{2W_k + \Sigma\big(h(x)\big)} \pmod{2^{k+1}}, \tag{14.1}$$

其中的困难是在上述迭代中, 求 $2W_k + \Sigma\big(h(x)\big)$ 在环 A^∞ 中的逆. 因 $h(x)|H(x)^D$, 故可令 $Q_H(x) := H(x)^D/h(x)$, 于是 $1/h(x) = Q_H(x)/H(x)^D$, 则有

$$\Big(2W_k + \Sigma\big(h(x)\big)\Big)^{-1} = \frac{Q_H(x)^2}{H(x)^{2D}\Big(1 + \frac{Q_H(x)^2(2W_k + \Sigma(h(x)) - h(x)^2)}{H(x)^{2D}}\Big)}. \tag{14.2}$$

注意到 $\Sigma\big(h(x)\big) \equiv h(x)^2 \pmod 2$, 可知上式右端分母是 A^∞ 中可逆元. 为了证明 $W := \lim_{k\to\infty} W_k \in A^\dagger$, 需要以下引理:

引理 14.1　对于 $k \geqslant 1$, 令

$$W_k = \sum_{i=-L_k}^{A_k} U_i(x)S(x)^i + \sum_{i=-L_k}^{B_k} V_i(x)S(x)^i y \in A,$$

其中 $S(x) = H(x)$ 或 x (如果 $\deg H > 0$ 或 $H(x) = 1$), 且 $\deg U_i < \deg S$, $\deg V_i < \deg S$, 设 W_k 满足

$$W_k^2 + \Sigma\big(h(x)\big)W_k - \Sigma\big(f(x)\big) \equiv 0 \pmod{2^k}, \quad W_k \equiv y^2 \pmod 2,$$

$$U_{A_k} \neq 0, \quad V_{B_k} \neq 0, \quad U_{-L_k} \neq 0 \text{ 或 } V_{-L_k} \neq 0,$$

且

$$U_i = 0 \text{ 或 } \mathrm{ord}_2\big(U_i(x)\big) < k, \quad \forall -L_k \leqslant i \leqslant A_k,$$

$$V_i = 0 \text{ 或 } \mathrm{ord}_2\big(V_i(x)\big) < k, \quad \forall -L_k \leqslant i \leqslant B_k,$$

则 A_k, B_k 和 L_k 满足

$$\begin{aligned} A_k &\leqslant 2(k-1)\big(d_S^f - 2d_S^h\big) + 2d_S^h, \\ B_k &\leqslant 2(k-2)\big(d_S^f - 2d_S^h\big) + \big(d_S^f - d_S^h\big), \\ L_k &\leqslant 4(k-1)D - 2D, \end{aligned} \tag{14.3}$$

其中 $d_S^f := \deg f/\deg S$, $d_S^h := \deg h/\deg S$.

证明 直接计算表明 $W_1 \equiv f(x) - h(x)y \pmod 2$, 故 $A_1 \leqslant d_S^f$, $B_1 \leqslant d_S^h$, $L_1 \leqslant 0$, 且

$$W_2 \equiv \frac{\Sigma\big(f(x)\big) - f(x)^2 - \Sigma\big(h(x)\big)f(x)}{h(x)^2} + y\frac{\Sigma\big(h(x)\big) + 2f(x)}{h(x)} \pmod 4,$$

这意味着 W_2 满足引理 14.1. 牛顿迭代 (14.1) 可重写为

$$h(x)^2W_{k+1} \equiv -W_k^2 + \big(h(x)^2 - \Sigma\big(h(x)\big)\big)W_k + \Sigma\big(f(x)\big) \pmod{2^{k+1}}. \tag{14.4}$$

令 $\alpha_k(x) := \sum_{i=-L_k}^{A_k} U_i(x)S(x)^i$, $\beta_k(x) := \sum_{i=-L_k}^{B_k} V_i(x)S(x)^i$, 使得 $W_k = \alpha_k(x) + \beta(x)y$, 注意到 $W_k \equiv W_{k-1} \pmod{2^{k-1}}$, 故可定义

$$\Delta_{\alpha,k}(x) := \frac{\alpha_k(x) - \alpha_{k-1}(x)}{2^{k-1}}, \quad \Delta_{\beta,k} := \frac{\beta_k(x) - \beta_{k-1}(x)}{2^{k-1}}, \qquad k \geqslant 1;$$

$$\Delta_{\alpha,0}(x) := \Delta_{\beta,0}(x) := 0.$$

于是有

$$W_k = \Delta_{\alpha,1} + 2\Delta_{\alpha,2} + \cdots + 2^{k-1}\Delta_{\alpha,k} + y\big(\Delta_{\beta,1} + 2\Delta_{\beta,2} + \cdots + 2^{k-1}\Delta_{\beta,k}\big).$$

将上式代入 (14.4) 式, 有

$$\begin{aligned} h(x)^2W_{k+1} \equiv &- \sum_{1\leqslant i<j, i+j-1<k+1} 2^{i+j-1}\big(\Delta_{\alpha,i}\Delta_{\alpha,j} + \big(f(x) - h(x)y\big)\Delta_{\beta,i}\Delta_{\beta,j}\big) \\ &- y\sum_{i+j-1<k+1} 2^{i+j-1}\Delta_{\alpha,i}\Delta_{\beta,j} \\ &- \sum_{2(i-1)<k+1} 2^{(i-1)}\big(\Delta_{\alpha,i}^2 + \big(f(x) - h(x)y\big)\Delta_{\beta,i}^2\big) \\ &+ \big(h(x)^2 - \Sigma\big(h(x)\big)\big)\sum_{i<k+1} 2^{i-1}\big(\Delta_{\alpha,i} + \Delta_{\beta,i}y\big) \\ &+ \Sigma\big(f(x)\big) \pmod{2^{k+1}}. \end{aligned}$$

但 $Q_H(x)h(x) = H(x)^D$, 故 $1/h(x)^2 = Q_H(x)^2/H(x)^{2D}$, $\deg Q_H = D\deg H - \deg h$, 又因为 $\deg\Delta_{\alpha,i} \leqslant A_i$, $\deg\Delta_{\beta,i} \leqslant B_i$, 从而 A_{k+1} 不大于

$$\begin{aligned} \max\Big(&\max_{i+j<k+2}\big(A_i + A_j, B_i + B_j + d_S^f\big), \\ &\max_{2i<k+3}\big(2A_i, 2B_i + d_S^f\big), \max_{i<k+1} A_i + 2d_S^h, 2d_S^f\Big) - 2d_S^h. \end{aligned}$$

再利用 (14.3) 式中 A_k 和 B_k 的上界及 $A_1 \leqslant d_S^f$, $B_1 \leqslant d_S^h$ 和 $L_1 \leqslant 0$. 我们看到 A_{k+1} 也满足 (14.3) 式所给出的上界. 类似地, 可以证明 B_{k+1} 和 L_{k+1} 也满足 (14.3) 式给出的上界, 证毕.

引理 14.1 表明可以将 q 次 Frobenius $\overline{F}$ 提升到 $A^\dagger$ 上的一个自同态 $\mathcal{F}$, 事实上, 由引理 14.1, 可以将 2 次 Fronenius σ 提升到 $A^\dagger$ 的一个自同态 Σ, 于是令 $\mathcal{F} := \Sigma^n$ 即可. 为了计算曲线 $\overline{C}$ 的 Zeta 函数, 需要决定 $\mathbb{Q}_q$ 向量空间 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 的一组基, 此处 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 是由微分复形 $(A^\dagger, d)$ 决定的上同调群的 "$-$" 特征子空间.

与奇特征的情形类似, 代数 de Rham 上同调 $H^1_{DR}(\mathcal{C}'_{f,h})$ 分裂为对合 l 的 2 个特征子空间之直和: 其中正特征子空间 $H^1_{DR}(\mathcal{C}'_{f,h})^+$ 由 $\left[\frac{x^i dx}{H(x)}\right]$ $(0 \leqslant i \leqslant s)$ 生成, 而负特征子空间 $H^1_{DR}(\mathcal{C}'_{f,h})^-$ 由 $x^i y dx (0 \leqslant i \leqslant 2g-1)$ 生成. 而正特征子空间对应于删除的分歧点 $(\theta_k, 0)(0 \leqslant k \leqslant s)$, 于是 $H^1_{DR}(\mathcal{C}'_{f,h})$ 中每个元素都可以写成微分 $x^k H(x)^m y^l dx$, $x^k H(x)^m y^l dy$ $(k, l \in \mathbb{N}, m \in \mathbb{Z})$ 的一个线性组合. 应用曲线方程, 可以约化到 $l = 0$ 或 1 的情形. 又因为 $d(x^k H(x)^m y)$ 和 $d(x^k H(x)^m y^2)$ 是正合微分, 故知道 $H^1_{DR}(\mathcal{C}'_{f,h})$ 由微分

$$x^k H(x)^m dx,\ x^k H(x)^m y dx, \quad k \in \mathbb{N}, m \in \mathbb{Z}$$

所生成.

显然, 对 $k \in \mathbb{N}, m \geqslant 0$, $x^k H(x)^m dx$ 是正合的, 若 $\deg H > 0$ 且 $m < 0$, 可以假定 $0 \leqslant k < \deg H$, 又因为 $H(x)$ 无平方因子, 可将 x^k 写成 $A(x)H(x) + B(x)H'(x)$ 的形式, 从而

$$x^k H(x)^m dx = A(x)H(x)^{m+1} dx + B(x)H'(x)H(x)^m dx, \tag{14.5}$$

因为 $d(B(x)H(x)^{m+1})$ 是正合的, 故可以利用关系

$$B(x)H'(x)H(x)^m dx \equiv -\frac{B'(x)H(x)^{m+1}}{m+1} dx \tag{14.6}$$

来更进一步约化 (14.5) 式的微分 (对 $m < -1$). (14.6) 式中的 "$\equiv$" 表示模去正合微分形式. 作为上述约化过程的结果, 我们可以将任意微分形式 $x^k H(x)^m dx$ 约化到微分形式 $x^i dx / H(x) (0 \leqslant i \leqslant s)$ 的一个线性组合.

如果知道如何约化微分形式 $x^i y dx (i \in \mathbb{N})$, 则我们就可以约化形式 $x^k H(x)^m y dx$ (对 $k \in \mathbb{N}$, $m > 0$). 将曲线 $\mathcal{C}$ 的方程重写如下:

$$\mathcal{C}:\ (2y + h(x))^2 = 4f(x) + h(x)^2,$$

并两端微分, 有

$$(2y + h(x))d(2y + h(x)) = (2f'(x) + h(x)h'(x))dx,$$

更进一步, 对所有 $j \geqslant 1$, 有

$$\begin{aligned} x^j\big(2f'(x)+h(x)h'(x)\big)\big(2y+h(x)\big)dx &= x^j\big(2y+h(x)\big)^2 d\big(2y+h(x)\big) \\ &\equiv -\frac{1}{3}\big(2y+h(x)\big)^3 dx^j \\ &\equiv -\frac{j}{3}x^{j-1}\big(4f(x)+h(x)^2\big)\big(2y+h(x)\big)dx. \end{aligned}$$

因为 $P(x)h(x)dx$(对任何 $P(x)\in\mathbb{Q}_q[x]$) 都是正合的, 故有

$$\Big[x^j\big(2f'(x)+h(x)h'(x)\big)+\frac{j}{3}x^{j-1}\big(4f(x)+h(x)^2\big)\Big]ydx \equiv 0, \tag{14.7}$$

括号中的多项式的次数为 $2g+j$, 其首项系数为 $2(2g+1)+\frac{4j}{3}\neq 0$, 注意上述公式对于 $j=0$ 也成立. 因此, 可以将任何 $x^iydx (i\geqslant 2g)$, 约化到形式 x^jydx, $j=i-2g$, 方法是将 x^iydx 减去 (14.7) 式左端一个适当的倍数即可. 继续这个过程, 可将任意 $x^iydx(i\geqslant 2g)$ 约化到 $x^iydx(0\leqslant i\leqslant 2g-1)$ 的一个线性组合.

对 $m<0$, 我们需要一个额外的方法以约化 $x^kH(x)^mydx\,(k\in\mathbb{N})$. 回忆 $Q_f(x)=f(x)/H(x)$, 因曲线 C 是非奇异的, 故 $(Q_f(x),H(x))=1$, 又因为 $H(x)$ 无重根, 故 $(H(x),Q_f(x)H'(x))=1$. 设 $i=-m>0$, 写 $x^k=A(x)H(x)+B(x)Q_f(x)H'(x)$, 则

$$\frac{x^k}{H(x)^i}ydx=\frac{A(x)}{H(x)^{i-1}}ydx+\frac{B(x)Q_f(x)H'(x)}{H(x)^i}ydx.$$

而上式右端第 2 个微分形式可利用下式约化:

$$\begin{aligned} \frac{B(x)}{H(x)^i}\big(2f'(x)+h(x)h'(x)\big)\big(2y+h(x)\big)dx &= \frac{B(x)}{H(x)^i}\big(2y+h(x)\big)^2 d\big(2y+h(x)\big) \\ &\equiv -\frac{1}{3}\big(2y+h(x)\big)^3 d\Big(\frac{B(x)}{H(x)^i}\Big), \end{aligned}$$

利用 $h(x)=Q_h(x)H(x), f(x)=Q_f(x)H(x)$ 和 $\big(2y+h(x)\big)^2=4f(x)+h(x)^2$, 得

$$\begin{aligned} \frac{B(x)Q_f(x)H'(x)}{H(x)^i}ydx \equiv{}& \frac{B\big(iH'Q_h^2-6Q_f'-3Q_hh'\big)-B'(4Q_f+Q_hh)}{(6-4i)H^{i-1}}ydx \\ &+\frac{I(x)}{H(x)}dx, \end{aligned}$$

此处, $I(x)dx/H(x)$ 是一个不变微分, 从而可以将任何一个微分形式

$$x^kH(x)^mydx,\quad k\in\mathbb{N}, m\in\mathbb{Z}$$

表成微分形式

$$x^iydx,\ 0\leqslant i\leqslant 2g-1,\qquad x^idx/H(x),\ 0\leqslant i\leqslant s$$

的一个线性组合.

为了证明上同调群 $H^1(\mathcal{C}'_{f,h})$ 的生成元集与 $H^1_{DR}(\mathcal{C}'_{f,h})$ 的生成元集相同 (参见定理 13.6 的证明), 我们需要界定上述约化过程中分母的赋值, 这就是下面的两个引理, 它们是第一章引理 13.1 和 13.2 的类似.

引理 14.2 设 $A := \mathbb{Z}_q[x,y]/(y^2 + h(x)y - f(x))$, 假设

$$x^r y dx = \sum_{i=0}^{2g-1} a_i x^i y dx + dS, \tag{14.8}$$

其中 $r \in \mathbb{N}, a_i \in \mathbb{Q}_q, S \in A \otimes \mathbb{Q}_q$, 则 $2^m a_i \in \mathbb{Z}_q, 2^{m'} S - \beta \in A$, 而 $m = 3 + \lfloor \log_2(r + g + 1) \rfloor$, $m' = 1 + m + \lfloor \log_2(2g + \deg(h)) \rfloor$, β 是 $\mathbb{Q}_q$ 中某个元素.

证明 分两部分, 第 1 部分类似于引理 13.2 的证明, 它基于在曲线 $\mathcal{C}$ 的无穷远点的局部分析. 令 $t = x^g/y$, 则易知

$$x = t^{-2}\left(1 + \sum_{j=1}^{\infty} \alpha_j t^j\right), \quad y = t^{-2g-1}\left(1 + \sum_{j=1}^{\infty} \beta_j t^j\right), \tag{14.9}$$

其中 $\alpha_i, \beta_j \in \mathbb{Z}_q$. 为此, 令 $z = \frac{1}{x}$, 则 $\mathcal{C}$ 的方程变为

$$z + tz^{g+1}h(1/z) - t^2 z^{2g+1} f(1/z) = 0.$$

利用上式和牛顿迭代, 就可以将 z 写成 t 的幂级数, 然后可得出 x 和 y 关于 t 的幂级数表达式 (14.9).

现在, (14.8) 式可重写为

$$2^{m-1} x^r \big(2y + h(x)\big) dx = \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i \big(2y + h(x)\big) dx + dT,$$

其中 $T \in A \otimes \mathbb{Q}_q$. 考虑 A 上的对合

$$l: \ x \mapsto x, \ 2y + h(x) \mapsto -(2y + h(x)),$$

可以写

$$T = \sum_{i=0}^{N} A_i x^i \big(2y + h(x)\big),$$

其中 N 足够大, $A_i \in \mathbb{Q}_q$. 于是

$$\begin{aligned} &2^{m-1} x^r \big(2y + h(x)\big) dx - \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i \big(2y + h(x)\big) dx \\ &= d\left(\sum_{i=0}^{N} A_i x^i \big(2y + h(x)\big)\right), \end{aligned} \tag{14.10}$$

将 (14.9) 式代入 (14.10) 式, 因为 $x^iy = t^{-2i-2g-1} + \cdots$, 故有

$$x^i\big(2y + h(x)\big)dx = \big(-4t^{-2i-2g-4} + \cdots\big)dt,$$

于是有

$$\begin{aligned}2^{m-1}\sum_{j\geqslant -\max(2r+2g+4,6g+2)}\gamma_j t^j dt = d\Bigg(&\sum_{i=0}^{N}2A_i\big(t^{-2i-2g-1}+\cdots\big)\\&+\sum_{i=0}^{N}A_i\big(ct^{-2i-2\deg(h)}+\cdots\big)\Bigg),\end{aligned}\tag{14.11}$$

其中 $\gamma_j \in \mathbb{Q}_q\,(\forall j)$, 且 $\gamma_j \in \mathbb{Z}_q$(对于 $j < -2(2g-1)-2g-4 = -6g-2$), c 是 $h(x)$ 的首项系数. 注意到 $c \in \mathbb{Z}_q$ 是单位, 关于 t 积分 (14.11) 式, 并除以 2 得

$$\begin{aligned}\sum_{j\geqslant -\max(2r+2g+3,6g+1)}\gamma'_j t^j = &\sum_{i=0}^{N}A_i\big(t^{-2i-2g-1}+\cdots\big)\\&+\sum_{i=0}^{N}\frac{A_i}{2}\big(ct^{-2i-2\deg(h)}+\cdots\big),\end{aligned}\tag{14.12}$$

其中 $\gamma'_j \in \mathbb{Q}_q\,(\forall j)$, $\gamma'_j \in \mathbb{Z}_q$(对于 $j < -6g-1$). 在积分时, 实际上出现了分母, 但若 $r \geqslant 2g-1$, 则乘上 $2^{\lfloor \log_2(2r+2g+2)\rfloor} = 2^{m-2}$ 后, 系数成为整数 (即在 $\mathbb{Z}_q$ 中). (14.12) 式的第一个结论是: 对于 $i > \max(r+1, 2g)$, 有 $A_i = 0$. 其次, (14.12) 式意味着对 $i > 2g$, 有 $A_i \in \mathbb{Z}_q$, 假设相反, 则存在一个最大的 i_0, 使得 $A_{i_0} \notin \mathbb{Z}_q$, 但 $i_0 > 2g$, 注意 $-2i_0 - 2g - 1 < -6g - 1$(否则 $i_0 \leqslant 2g$), 故 (14.12) 式左端次数不大于 $-2i_0 - 2g - 1$ 的单项式的系数属于 $\mathbb{Z}_q$. 更进一步, 由 i_0 的定义, 在 (14.12) 式右端第一个和式中的次数小于 $-2i_0 - 2g - 1$ 的单项式的系数也在 $\mathbb{Z}_q$ 中. 而其中次数为 $-2i_0 - 2g - 1$ 的单项式的系数不在 $\mathbb{Z}_q$ 中. 因此 (14.12) 式右端中第二个和式也包含一个次数为 $-2i_0 - 2g - 1$ 的单项式, 其系数不属于 $\mathbb{Z}_q$. 因此, 存在一个最大的 i_1, 使得 $A_{i_1}/2 \notin \mathbb{Z}_q$ 且 $-2i_1 - 2\deg(h) \leqslant -2i_0 - 2g - 1$. 但 $-2i_1 - 2\deg(h)$ 为偶数, 故 $-2i_1 - 2\deg(h) < -2i_0 - 2g - 1$. 因为 $c \in \mathbb{Z}_q$ 是单位, (14.12) 式右端有一个次数为 $-2i_1 - 2\deg(h) < -2i_0 - 2g - 1$ 的单项式, 其系数不属于 $\mathbb{Z}_q$. 但 (14.12) 式左端数不大于 $-2i_0 - 2g - 1$ 的单项式的系数均属于 $\mathbb{Z}_q$, 这是一个矛盾, 从而 $A_i \in \mathbb{Z}_q\,(\forall i > 2g)$.

现在考虑证明的第二部分. 注意到 $\big(2y + h(x)\big)^2 = 4f(x) + h(x)^2 := v(x)$, 及 $d\big(2y + h(x)\big) = \frac{w(x)}{2y+h(x)}dx$, $w(x) := 2f'(x) + h(x)h'(x)$. 我们将利用这些关系式将 (14.10) 式约化为不含 y 的关系式. 将 (14.10) 式两端乘以 $\frac{2y+h(x)}{dx} = \frac{w(x)}{d\left(2y+h(x)\right)}$,

有

$$2^{m-1}x^r v(x) - \sum_{i=0}^{2g-1} 2^{m-1}a_i x^i v(x) = \sum_{i=0}^{N} A_i i x^{i-1} v(x) + \sum_{i=0}^{N} A_i x^i w(x),$$

将上式改写成

$$\left(\sum_{i=0}^{2g-1} 2^{m-1}a_i x^i\right) v(x) + \left(\sum_{i=0}^{2g} A_i i x^{i-1}\right) v(x) + \left(\sum_{i=0}^{2g} A_i x^i\right) w(x) = F(x), \quad (14.13)$$

其中

$$F(x) := 2^{m-1}x^r v(x) - \sum_{i=2g+1}^{N} A_i i x^{i-1} v(x) - \sum_{i=2g+1}^{N} A_i x^i w(x) \quad (14.14)$$

是 $\mathbb{Z}_q$ 上的多项式 (因为对于 $i > 2g$, 有 $A_i \in \mathbb{Z}_q$), 由 (14.13) 和 (14.14) 式知 $\sum_{i=0}^{2g} A_i \theta_k^i$ 具有赋值不小于 0, 这是因为对于 $H(x)$ 的每一个根 θ_k, 有 $v(\theta_k) = 0$, $w(\theta_k) \neq 0$. 为了去掉 $w(x)$ 的定义中的因子 2, 考虑多项式

$$q(x) := h'(x)H(x)/h(x) \in \mathbb{Z}_q[x],$$
$$u(x) := \frac{1}{2}\big(w(x) - q(x)v(x)/H(x)\big) = f'(x) - 2q(x)f(x)/H(x),$$

则 $u(x) \in \mathbb{Z}_q[x]$, $\deg q(x) = \max(0, \deg(H) - 1)$, $\deg(u) = 2g$ 且 $u(x)$ 的首项系数为 $\mathbb{Z}_q$ 中的单位. 将 (14.13) 式改写为

$$\left(\sum_{i=0}^{2g-1} 2^{m-1}a_i x^i + \sum_{i=0}^{2g} A_i i x^{i-1} + \frac{q(x)}{H(x)} \sum_{i=0}^{2g} A_i x^i\right) v(x) + \left(\sum_{i=0}^{2g} 2A_i x^i\right) u(x) = F(x), \quad (14.15)$$

令 $q(x)\sum_{i=0}^{2g} A_i x^i = H(x)B(x) + B_H(x)$, $\deg(B_H) < \deg(H)$, $B_H \in \mathbb{Q}_q[x]$. 因对 $H(x)$ 的每一个根 θ_k, $\sum_{i=0}^{2g} A_i \theta_k^i$ 具有赋值不小于 0, 故 $B_H(\theta_k)$ 具有赋值不小于 0(因 $H(\theta_k) = 0$), 从而 $B_H(x) \in \mathbb{Z}_q[x]$(因为 $H(x)$ 的判别式是 $\mathbb{Z}_q$ 中的单位), 于是

$$\left(\sum_{i=0}^{2g-1} \left(2^{m-1}a_i + (i+1)A_{i+1} + B_i\right) x^i\right) v(x) + \left(\sum_{i=0}^{2g} 2A_i x^i\right) u(x)$$
$$= F(x) - \frac{B_H(x)v(x)}{H(x)}, \quad (14.16)$$

其中 B_i 是 $B(x)$ 的 i 次系数, 即 $B(x) = \sum_{i=0}^{2g-1} B_i x^i$. 将 (14.16) 式视为未知量 $(2^{m-1}a_i + (i+1)A_{i+1} + B_i)$ $(0 \leqslant i \leqslant 2g)$ 和 $2A_i$ $(1 \leqslant i \leqslant 2g)$ 的线性方程组, 则其系数行列式为 $v(x)$ 和 $u(x)$ 的结式 $\mathrm{Res}(v(x), u(x))$(注意 $\deg(v) = 2g+1$, $\deg(u) = 2g$). 因为对 $u(x)$ 的每一个根 ξ, $v(\xi)$ 的赋值是零 (这是由于 $f'(x)$ 和 $h(x)$ 的结式是一个

单位), 故 $\mathrm{Res}(v(x),u(x))$ 是 $\mathbb{Z}_q$ 中的单位. 从而上述线性方程组 (14.16) 的解属于 $\mathbb{Z}_q$, 即 $2A_i \in \mathbb{Z}_q$, $2^{m-1}a_i + (i+1)A_{i+1} + B_i \in \mathbb{Z}_q$. 由 B_i 的定义, 知 $2B_i \in \mathbb{Z}_q$(因为 $2A_i \in \mathbb{Z}_q$, $B_H(x) \in \mathbb{Z}_q[x]$), 从而 $2^m a_i \in \mathbb{Z}_q$. 这就完成了引理的证明.

引理 14.3 设 $A := \mathbb{Z}_q[x,y,H(x)^{-1}]/(y^2 + h(x)y - f(x))$, $\deg(h) > 0$ 且假定

$$\frac{B(x)}{H(x)^r} y dx = \sum_{i=0}^{2g-1} a_i x^i y dx + \sum_{i=0}^{s} \frac{b_i x^i}{H(x)} dx + dS, \tag{14.17}$$

此处 $r \in \mathbb{N}$, $B(x) \in \mathbb{Z}_q[x]$, $\deg(B) < \deg(H)$, $a_i, b_i \in \mathbb{Q}_q$ 且 $S \in A \otimes \mathbb{Q}_q$, 则 $2^m a_i \in \mathbb{Z}_q$, $2^{m'} b_i \in \mathbb{Z}_q$, $2^{m'} S - \beta \in A$, 其中 $m = 3 + \lfloor \log_2(r+1) \rfloor$, $m' = 1 + m + \lfloor \log_2(2g + \deg(h)) \rfloor$ 且 β 是 $\mathbb{Q}_q$ 中某个元素.

证明 方法与引理 14.2 类似. 但此时我们考虑在分歧点 $(\theta_k, 0)(0 \leqslant k \leqslant s)$ 处的局部分析. 此时 y 是 $(\theta_k, 0)$ 处的局部坐标. 曲线在 $(\theta_k, 0)$ 的局部环的完备化下, 有

$$x - \theta_k = \gamma_{k,2} y^2 + \sum_{j \geqslant 3} \gamma_{k,j} y^j, \tag{14.18}$$

此处 $\gamma_{k,j} \in \mathbb{Z}_q^{ur}$ 而 $\gamma_{k,2} \in \mathbb{Z}_q^{ur}$ 是单位. 为了看出这些事实, 只要将 $h(x)$ 和 $f(x)$ 在 θ_k 处泰勒展开, 然后应用曲线方程和条件 $f'(\theta_k) \neq 0 \pmod 2$, 以及牛顿迭代, 就可以将 $x - \theta_k$ 表示成 y 的幂级数如上. 应用对合 l 到 (14.17) 式, 可知该式意味着

$$\begin{aligned} &2^{m-1} B(x) H(x)^{-r} (2y + h(x)) dx - \sum_{i=0}^{2g-1} 2^{m-1} a_i x^i (2y + h(x)) dx \\ =& d\left(\sum_{i=-N}^{M} B_i(x) H(x)^i (2y + h(x)) \right), \end{aligned} \tag{14.19}$$

其中 N 和 M 是足够大的整数. 由 (14.18) 式, 有

$$B_i(x) H(x)^i = u_{k,i} B_i(\theta_k) y^{2i} + \cdots, \qquad u_{k,i} \in \mathbb{Z}_q^{ur} \text{为单位}.$$

将此带入 (14.19) 式, 并除以 2, 得

$$\begin{aligned} 2^{m-2} \sum_{j \geqslant -2r+2} \gamma'_{k,j} y^j dy =& d\left(\sum_{i=-N}^{M} \left(u_{k,i} B_i(\theta_k) y^{2i+1} + \cdots \right) \right) \\ &+ d\left(\frac{u_{k,i} B_i(\theta_k)}{2} \cdot \frac{\gamma_{k,2}^{m_k} h^{(m_k)}(\theta_k)}{m_k!} y^{2i+2m_k} + \cdots \right), \end{aligned} \tag{14.20}$$

其中 $\gamma'_{k,j} \in \mathbb{Q}_q^{ur} (\forall j)$, $\gamma'_{k,j} \in \mathbb{Z}_q^{ur}$(若 $j \leqslant 1$). 积分上式左端 (关于 y), 得到一个级数, 其次数不大于 2 的项之系数属于 $\mathbb{Z}_q^{ur}$. 而右端的首项是 $u_{k,-N} B_{-N}(\theta_k) y^{-2N+1}$,

这意味着 $B_{-N}(\theta_k)\,(0 \leqslant k \leqslant s)$ 是整的. 但 $H(x)$ 的判别式是 $\mathbb{Z}_q$ 中的单位, 故 $B_{-N}(x)$ 具有整系数. 将此整系数项移至 (14.20) 式左端, 然后重复上述过程, 可证明 $B_i(x) \in \mathbb{Z}_q[x]$, $-N \leqslant i \leqslant 0$. 下面的证明步骤与引理 14.2 的类似. 首先将和式

$$\sum_{i=1}^{M} B_i(x)H(x)^i\big(2y+h(x)\big)$$

改写为如下形式:

$$\sum_{i=0}^{M'} A_i x^i\big(2y+h(x)\big), \quad M' \in \mathbb{N},\ A_i \in \mathbb{Q}_q.$$

将 $\frac{2y+h(x)}{dx} = \frac{w(x)}{d(2y+h(x))}$ 乘到 (14.19) 式两端, 有

$$\begin{aligned}
&2^{m-1}\frac{B(x)}{H(x)^r}v(x) - \sum_{i=0}^{2g-1} 2^{m-1}a_i x^i v(x)\\
=&\sum_{i=-N}^{0} B_i(x)H(x)^i w(x) + \sum_{i=0}^{M'} A_i x^i w(x) + \sum_{i=-N}^{0}\big(B_i(x)iH(x)^{i-1}H'(x)\\
&+B_i'(x)H(x)^i\big)v(x) + \sum_{i=0}^{M'} A_i i x^{i-1} v(x).
\end{aligned} \tag{14.21}$$

比较两端在无穷远处的赋值, 表明 $A_i = 0$(对 $i > 2g$), 故上式可改写为如下形式:

$$\left(\sum_{i=0}^{2g-1} 2^{m-1}a_i x^i\right)v(x) + \left(\sum_{i=0}^{2g} A_i i x^{i-1}\right)v(x) + \left(\sum_{i=0}^{2g} A_i x^i\right)w(x) = F(x), \tag{14.22}$$

其中

$$\begin{aligned}
F(x) = 2^{m-1}\frac{B(x)}{H(x)^r}v(x) &- \sum_{i=-N}^{0} B_i(x)H(x)^i w(x)\\
&- \sum_{i=-N}^{0}\big(B_i(x)iH(x)^{i-1}H'(x) + B_i'(x)H(x)^i\big)v(x)
\end{aligned}$$

是 $\mathbb{Z}_q$ 上的多项式 (因为 $B_i(x) \in \mathbb{Z}_q[x]$, $-N \leqslant i \leqslant 0$), 而 (14.22) 式左端也是一个多项式, 由 A_i 的定义知 $H(x)|\sum_{i=0}^{2g} A_i x^i$. 现在完全类似引理 14.2 相应部分的证明 (但此时 $B_H(x) = 0$), 知 $2^m a_i \in \mathbb{Z}_q$ 从而引理得证.

注记 14.1 如果 $r = 0$, 则上面的证明中, $B_i(x) = 0\,(\forall i \leqslant 0)$, 且对于 $0 \leqslant i \leqslant 2g-1$, a_i 由 (14.22) 式完全决定 (通过考虑结式). 这就证明 $x^i y dx (0 \leqslant i \leqslant 2g-1)$ 和 $\frac{x^i}{H(x)}dx (0 \leqslant i \leqslant s)$ 是 $H^1_{DR}(C'_{f,h})$ 中线性无关的元素.

上面引理 14.2 和 14.3 表明 $H^1_{DR}(\mathcal{C}'_{f,h})$ 的基 $\{x^i y dx, \frac{x^i}{H(x)}dx\}$ 是 $H^1(\mathcal{C}'_{f,h})$ 的一个生成元集合 (因为约化过程是收敛的). 事实上, 若 $\sum_{k,l} a_{k,l}x^k S(x)^l y \in A^\dagger(k,l \in \mathbb{Z}, 0 \leqslant k < \deg S)$, $a_{k,l}$ 的赋值的增长是 $|l|$ 的线性函数, 而在约化过程中出来的分母的赋值仅仅是 $|l|$ 的对数.

最后, 由定理 13.4, 知只要计算出 Frobenius $\mathcal{F}_q$ 在 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 上的矩阵, 就可以计算出曲线 $\overline{C}$ 的多项式 $P_{\overline{C}}$ 了.

§14.2 算法综述

在本节中, 我们将上节中的理论分析描述成一个具体的算法, 以计算 $\mathbb{F}_q$ 上任意一条光滑的亏格 g 的超椭圆曲线 $\overline{C}$ 的 Frobenius 的特征多项式 $P_{\overline{C}}$ 和 Zeta 函数.

由于 $P_{\overline{C}}(t) = t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g}$ 是 $\mathcal{F}_q$ 在 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 上的特征多项式, 而 Weil 猜想表明 $q^{g-i}a_i = a_{2g-i}$, 故只要计算 $a_1, \cdots, a_g$ 即可. 又由于对 $1 \leqslant i \leqslant g$, 有

$$|a_i| \leqslant \binom{2g}{i} q^{i/2} \leqslant \binom{2g}{g} q^{q/2} \leqslant 2^{2g} q^{g/2},$$

故只要计算 $\mathcal{F}_q$ 在 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 的一组基上的作用 (模 2^B) 即可, 其中

$$B \geqslant \left\lceil \log_2(2\binom{2g}{g} q^{g/2} \right\rceil.$$

但仅仅计算 $\sum(y) \pmod{2^B}$ 并不够, 因为在微分形式的约化过程中, 精度可能降低. 设 $\sum(y) \equiv \alpha_N + \beta_N y \pmod{2^N}$, 令 $\beta_N = \sum_{i=-L_N}^{B_N} V_i(x)S(x)^i$, 则引理 14.1 表明

$$L_N \leqslant 4(N-1)D - 2D, \quad B_N \leqslant 2(N-2)(d_S^f - 2d_S^h) + (d_S^f - d_S^h), \tag{14.23}$$

由于我们要约化形式 $x^{2i+1}\sum(y)dx (0 \leqslant i \leqslant 2g-1)$, 故降低的精度由

$$x^{4g-1} V_{B_N}(x) S(x)^{B_N} y dx, \quad x V_{-L_N}(x) S(x)^{-L_N} dx$$

的约化所决定. 直接计算表明出现在前一个微分形式中的 x 的最高幂次不超过 $2N(\deg f - 2\deg h) + bg$, 而引理 14.2 表明约化它所降低的精度由下式界定:

$$C_{N,1} := 3 + \lfloor \log_2 2N(\deg f - 2\deg h) + 7g + 1 \rfloor.$$

类似地, 引理 14.3 表明约化后一个微分形式所降低的精度由下式界定:

$$C_{N,2} := 3 + \lfloor \log_2(4ND - 6D + 1) \rfloor.$$

于是只要计算 $\bmod 2^N$ 即可, 其中

$$N - \max(C_{N,1}, C_{N,2}) > B, \tag{14.24}$$

我们可叙述算法如下:

(算法 14.1) Hyper-Zeta

输入: 一条 $\mathbb{F}_q$ 上超椭圆曲线 $\overline{C}$: $y^2 + \overline{h}(x)y = \overline{f}(x)$, $q = 2^n$.

输出: $\widetilde{C}$ 的 Zeta 函数 $Z(\widetilde{C}/\mathbb{F}_q; t)$.

Step 1: $B \geqslant \lceil \log_2(2\binom{2g}{g}q^{g/2}) \rceil$, $N - \max(C_{N,1}, C_{N,2}) > B$;

Step 2: $(h(x), f(x), H(x), D) = \text{Lift_Curve}(\overline{h}(x), \overline{f}(x))$;

Step 3: $\alpha_N, \beta_N = \text{Lift_Frob_y}(h, f, H, D, N)$;

Step 4: 对于 $i = 0$ 到 $2g-1$, 计算

4.1 $R_i(x) = \text{Red_Cohomology}(2x^{2i+1}\beta_N, h, f, H, N)$;

4.2 对 $j = 0$ 到 $2g-1$, 计算 $M[i][j] = \text{Coeff}(R_i, j)$;

Step 5: $M_{\mathcal{F}_q} = \Sigma^{n-1}(M) \cdots \Sigma(M)M \pmod{2^B}$;

Step 6: $\chi(t) = \text{Character_Poly}(M_{\mathcal{F}_q}) \pmod{2^B}$;

Step 7: 对 $i = 0$ 到 g, 计算

7.1 若 $\text{Coeff}(\chi, 2g-i) > \binom{2g}{i}q^{i/2}$, 则

$$\text{Coeff}(\chi, 2g-i) -= 2^B;$$

7.2 $\text{Coeff}(\chi, i) = q^{g-i}\text{Coeff}(\chi, 2g-i)$;

Step 8: 输出 $Z(\widetilde{C}/\mathbb{F}_q; t) = \frac{t^{2g}\chi(1/t)}{(1-t)(1-qt)}$.

(算法 14.2) Lift_Frob_y

输入: 曲线 $C/\mathbb{Z}_q$: $y^2 + h(x) = f(x)$, $H \in \mathbb{Z}_q[x]$, $H|h$, $H|f$, $D \in \mathbb{N}$ 使 $h|H^D$, 精度为 N.

输出: S 的 Laurent 多项式 α_N, β_N, 其中 $S = x$ 或 H(按照 $H = 1$ 或 $\deg H > 0$), 使得 $\Sigma(y) \equiv \alpha_N + \beta_N y \pmod{2^N}$.

Step 1: $B = \lceil \log_2 N \rceil + 1$, $T = N$, $Q_S := S^D$ 除以 h 的商;

Step 2: 对 $i = B$ 到 1, 计算 $P[i] = T$, $T = \lceil T/2 \rceil$;

Step 3: $\alpha \equiv f \pmod 2$, $\beta \equiv -h \pmod 2$; $\gamma = 1$; $\delta = 0$;

Step 4: 对于 $i = 2$ 到 B, 计算

4.1 $T_A \equiv \big((\alpha + \Sigma(h)) \cdot \alpha + \beta^2 \cdot f - \Sigma(f)\big) \cdot Q_S^2 \cdot S^{-2D} \pmod{2^{P[i]}}$;

4.2 $T_B \equiv \big(2\alpha - h \cdot \beta + \Sigma(h)\big) \cdot \beta \cdot Q_S^2 \cdot S^{-2D} \pmod{2^{P[i]}}$;

4.3 $D_A \equiv 1 + \big(\Sigma(h) - h^2 + 2\alpha\big) \cdot Q_S^2 \cdot S^{-2D} \pmod{2^{P[i-1]}}$;

4.4 $D_B \equiv 2\beta \cdot Q_S^2 \cdot S^{-2D} \pmod{2^{P[i-1]}}$;

4.5 $V_A \equiv D_A \cdot \gamma + D_B \cdot \delta \cdot f - 1 \pmod{2^{P[i-1]}}$;

4.6 $V_B \equiv D_A \cdot \delta + D_B \cdot (\gamma - \delta \cdot h) \pmod{2^{P[i-1]}}$;

4.7 $\gamma \equiv \gamma - (V_A \cdot \gamma + V_B \cdot \delta \cdot f) \pmod{2^{P[i-1]}}$;

4.8 $\delta \equiv \delta - (V_A \cdot \delta + V_B \cdot (\gamma - \delta \cdot h)) \pmod{2^{P[i-1]}}$;

4.9 $\alpha \equiv \alpha - (T_A \cdot \gamma + T_B \cdot \delta \cdot f) \pmod{2^{P[i]}}$;

4.10 $\beta \equiv \beta - (T_A \cdot \delta + T_B \cdot (\gamma - \delta \cdot h)) \pmod{2^{P[i]}}$;

Step 5: 输出 $\alpha_N = \alpha$, $\beta_N = \beta$.

(算法 14.3) Red_Cohomology

输入: $h, f, H \in \mathbb{Z}_q[x], H|h, H|f, H$ 首一, $G = \sum_i T_i(x)S(x)^i$ 为 Laurent 多项式, $T_i \in \mathbb{Z}_q[x], \det T_i < \deg S$, $B \in \mathbb{N}, S(x) = x$ 或 H(按照 $H = 1$ 或 $\deg H > 0$).

输出: $\Lambda \in \mathbb{Q}_q[x]$, 使 $\deg \Lambda < 2g$ 且 $\Lambda y dx \sim G y dx \pmod{2^B}$.

Step 1: $N - \max(C_{N,1}, C_{N,2}) > B$;

Step 2: $Q_f = f$ 除以 S 的商, $Q_h = h$ 除以 S 的商, $P = 0$, $V = 0$, $v_G = \mathrm{Val}(G)$;

Step 3: 对于 $i = v_G$ 到 -1,

3.1 $V \equiv P + \mathrm{coeff}(G, i) \pmod{2^N}$;

3.2 $P \equiv V$ 除以 S 的商 $\mathrm{mod} 2^N$, $V \equiv V - P \cdot S \pmod{2^N}$;

3.3 $(C, L_A, L_B) = \mathrm{XGCD}(S, Q_f \cdot S', N)$;

3.4 $L_A = V \cdot L_A \pmod{2^N}$, $L_B = V \cdot L_B \pmod{2^B}$;

3.5 $P \equiv P + L_A$
$$+\frac{L_B \cdot (-iQ_h^2 \cdot S' - 3(2Q_f' + Q_h \cdot h')) - L_B'(4Q_f + Q_h \cdot h)}{6 + 4i} \pmod{2^N};$$

Step 4: $d_G = \mathrm{degree}(G)$; $d_T = (d_G + 1)\mathrm{degree}(S)$; $T = 0$;

Step 5: 对于 $i = d_G$ 到 0, 计算

$$T = T \cdot S + \mathrm{Coeff}(G, i) \pmod{2^N}; \quad T = T + P;$$

Step 6: 对于 $i = d_T$ 到 $2g$, 计算

6.1 $P \equiv x^{i-2g}\big(2f' + h \cdot h'\big) + \frac{i-2g}{3} x^{i-2g-1}\big(4f + h^2\big) \pmod{2^N}$;

6.2 $T \equiv T - \big(\text{Coeff}(T,i)\cdot P\big)/\text{Coeff}(P,i) \pmod{2^N}$;

Step 7: 输出 $\Lambda \equiv T \pmod{2^B}$.

我们对上述 3 个算法说明如下：在算法 14.1 中, 函数 hyper-Zeta 计算一条光滑射影超椭圆曲线 $\widetilde{C}$ 的 zeta 函数, 其中第 1 步决定满足 (14.24) 式的最小精度. 第 2 步, 称之为 Lift-Curve, 它是由 §14.1 刚开始所描述的提升所构造出来的：首先构造一同构曲线, 使得 $\overline{H}(x)|\overline{h}(x)$, $\overline{H}(x)|\overline{f}(x)$, 然后再利用 §14.1 刚开始的描述构造 $\mathbb{Z}_q$ 上的一超椭圆曲线 C : $y^2 + h(x)y = f(x)$, 以及一个多项式 $H(x)$, 整数 D, 使得 $H(x)|h(x)$, $h(x)|H(x)^D$. 在第 3 步, 计算 $\Sigma(y) \pmod{2^N}$, 这时我们应用算法 14.2 中的函数 Lift_Frob_y 来完成此任务. 参数 α_N 和 β_N 是 S 的 Laurent 多项式 (系数是 $\mathbb{Z}_q/(2^N\mathbb{Z}_q)$ 上次数小于 $\deg(S)$ 的多项式). 这个函数实现了牛顿迭代 (14.1) 式. 注意算法 14.2 实际上是一个双重牛顿迭代：$\alpha + \beta y$ 收敛到 $\Sigma(y)$, 而 $\gamma + \delta y$ 是牛顿迭代 (14.1) 式的分母的逆的一个近似值. 在我们获得 $\Sigma(y)$ 的近似值后, 就要计算 Σ 在 $H^1(\mathcal{C}'_{\overline{f},\overline{h}})^-$ 的基 $\{2x^{2i+1}\Sigma(y)\}_{0\leqslant i\leqslant 2g-1}$ 上的作用. 在第 4 步, 我们就是约化这些微分形式. 此时应用算法 14.3 中的函数 Red_Cohomology, 它是基于我们在 §14.1 中所叙述的约化过程而写成的. 对于给定的一个微分形式 $Gydx$(G 是关于 S 的一个 Laurent 多项式), 函数 Red-Cohomology 计算出一个多项式 $\Lambda \in \mathbb{Q}_q[x]$, 使得 $\deg(\Lambda) < 2g$ 且 $\Lambda ydx \sim Gydx \pmod{2^B}$. 在算法 14.3 的第 3.3 步中, 我们用到了函数 XGCD, 即所谓的广义欧氏除法, 对于输入的两个多项式 $A(x)$ 和 $B(x)$, XGCD 将给出多项式 $C(x), L_A(x), L_B(x)$, 使得 $C(x) = \gcd\big(A(x), B(x)\big)$ 且 $C(x) = L_A(x)A(x) + L_B(x)B(x)$. 由引理 14.2 和 14.3 知, 算法 14.3 的结果是正确的 $\pmod{2^N}$, 因为我们的计算是 $\bmod 2^N$ 的, 而 N 满足 $N - \max(C_{N,1}, C_{N,2}) > B$. 现在算法 14.1 中第 4 步给出了矩阵 $M \bmod 2^B$ 的值, 而在第 5 步, 我们算出了 M 的范 (Norm): $M_{\mathcal{F}} = \Sigma^{n-1}(M)\cdots\Sigma(M)M \pmod{2^B}$, 第 6 步和第 7 步是计算矩阵 $M_{\mathcal{F}}$ 的特征多项式, 第 8 步是输出一条光滑射影超椭圆曲线 $\widetilde{C}$ 的 zeta 函数, 其中 $\widetilde{C}$ 双有理等价于 $\overline{C}$.

与奇特征时 Kedlaya 算法类似, 我们不难给出现在的算法所需的时间复杂度和存储空间, 可以总结如下：

定理 14.1 *存在一个计算定义在有限域 $\mathbb{F}_{2^n}$ 上的亏格为 g 的光滑超椭圆曲线的 zeta 函数的确定型算法, 其时间复杂度为*

$$O\big(g^3n^3(g + (\log n)^2 \log\log n)\log(gn)\log\log(gn)\big),$$

而所需存储空间平均而言为 $O(g^3n^3)$, 在最坏的情形则为 $O(g^4n^3)$.

第四部分

椭圆曲线密码体制的攻击方法

第十五章　椭圆曲线离散对数的初等攻击

§15.1　椭圆曲线公钥密码

以下通过椭圆曲线公钥密码来说明这个概念及其应用.

设 E 为定义在有限域 $\mathbb{F}_q$ 上的椭圆曲线, 为简单起见, 以下假定 $q \neq 2,3$ 为一素数. 在 $E(\mathbb{F}_q)$ 中选一个点 P, 称为基点, 记 P 的阶为 n, 通常要求 n 是一个大素数 (其理由见 §15.2). 每个用户选取一个整数 e $(1 \leqslant e < n)$ 作为其私钥, 而以点 $D = eP$ 作为其公钥, 这样就形成一个椭圆曲线公钥密码系统 (ECC). 定义 E 的方程 $y^2 = x^3 + ax + b$ $(4a^3 + 27b^2 \neq 0)$, 基域 $\mathbb{F}_q$ 和基点 P 及其阶 n, 以及每个用户的公钥都是该系统的公开参数. 每个用户的私钥都是保密的, 仅本人知道.

假设用户 A 欲将明文 m $(0 < m < q)$ 加密后发送给 B, A 首先要查得 B 的公钥 D_B, 然后进行以下的加密运算:

1. 取随机数 $k \in \mathbb{Z}$ 计算 $kP = (x_1, y_1)$(今后将 $[k]P$ 简写为 kP);
2. 计算 $kD_B = (x_2, y_2)$;
3. 计算密文 $c = m \oplus x_2$(将 m 和 x_2 用二进制表示, 然后按位模 2 加), 将 (c, x_1, y_1) 发送给 B.

B 收到 A 发来的信息后, 进行下述的运算:

1. 计算 $e_B(x_1, y_1) = (x_2, y_2)$, e_B 为 B 的私钥;
2. 计算 $m = c \oplus x_2$, 得到明文 m.

因为 $e_B(x_1, y_1) = e_BkP = kD_B = (x_2, y_2)$, 上述解密是正确的.

公钥密码另一个重要用途是进行数字签名. 在计算机网络通信中, 数字签名可用于确认发信人的身份; 发现在传输过程中, 信息 m 是否被非法篡改; 具有不可抵赖不可更改性. 以下介绍基于椭圆曲线的数字签名方案 (ECDSA).

假设用户 A 对信息 m(为简单起见, 这里不妨假设 $0 < m < q$) 作数字签名, A 随机选取 $k \in \mathbb{Z}$, 计算 kP, 令 $r = x(kP)$ (kP 的 x 坐标), 计算 s, 它适合

$$sk \equiv m + re_A \mod n$$

(e_A 是 A 的私钥), 则 (m, r, s) 就是签名后 A 发出的报文.

任一用户收到 A 发出的 (m, r, s), 查得 A 的公钥 D_A, 计算 $s^{-1} \mod n$, 检验

$$r = x(s^{-1}(mP + rD_A))$$

是否成立, 如果成立, 签名得到验证; 否则, 不能通过验证. 由于 $skP = mP + re_AP = mP + rD_A$, 所以 $kP = s^{-1}(mP + rD_A)$, 上述验证显然是正确的. 只有 A 才知道他的私钥 e_A, 任何第 3 者要假冒 A 的签名, 或更改经 A 签名后的信息, 都是难于通过验证的. A 对信息签名后, 也是不能否认的.

已知 E 的点 D 是 P 的倍数, 求 $l \in \mathbb{Z}$, 使得 $D = lP$, 这称为椭圆曲线的离散对数问题 (ECDLP). ECC 的安全性是建立在离散对数计算难度基础之上, 如果离散对数可以计算, 从一个用户的公钥就可得到他的私钥, ECC 就不安全了. 本章集中研究离散对数的计算问题.

在应用椭圆曲线公钥密码时, 最主要的计算量用于计算 kP. 今以 $\mathbb{F}_p(p > 3$ 为素数) 上的椭圆曲线为例, 说明如何计算 kP. 椭圆曲线上的点可以用射影坐标 (X, Y, Z) 或仿射坐标 $x = X/Z, y = Y/Z$ 表示, 现在再引进一个新的坐标 (称为 Jacobi 坐标), 令 $x = X/Z^2, y = Y/Z^3$, 它适合方程

$$Y^2 = X^3 + aXZ^4 + bZ^6,$$

该方程与齐次形式

$$Y^2Z = X^3 + aXZ^2 + bZ^3$$

显然定义同一条曲线. 以下将会看到, 使用不同的坐标, 计算椭圆曲线上两点之和 $P + Q$ 与倍点 $2P$ 的计算量是不同的. 以 S, M, I 分别表示 $\mathbb{F}_p$ 中进行一次平方运算, 乘法运算和求逆运算所需的时间 (几乎对所有的域 $\mathbb{F}_p$, S 约为 $0.8M$, 而 I/M 随着基域 $\mathbb{F}_p$ 的不同, 以及算法实现的不同而有所变化, 当 $|p| > 100$ 比特时, 估计 I/M 在 9.5 与 30 之间).

仿射坐标下加法的计算公式. 令 $P = (x_1, y_1), Q = (x_2, y_2)$ 及 $P + Q = (x_3, y_3)$, 当 $P \neq Q$ 时, 加法公式为

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda(x_1 - x_3) - y_1,$$

其中 $\lambda = (y_2 - y_1)/(x_2 - x_1)$.

当 $P = Q$ 时, 倍点公式为

$$x_3 = \lambda^2 - 2x_1, \qquad y_3 = \lambda(x_1 - x_3) - y_1,$$

其中 $\lambda = (3x_1^2 + a)/(2y_1)$. 易见在仿射坐标下加法运算和倍点运算所需计算量分别为 $I + 2M + S$ 和 $I + 2M + 2S$.

考虑使用射影坐标时所需计算量, 令 $P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$ 及 $P + Q = (X_3, Y_3, Z_3)$, 当 $P \neq \pm Q$ 时, 容易推得其加法公式为

$$X_3 = vA, \quad Y_3 = u(v^2X_1Z_2 - A) - v^3Y_1Z_2, \quad Z_3 = v^3Z_1Z_2,$$

其中 $u = Y_2Z_1 - Y_1Z_2$, $v = X_2Z_1 - X_1Z_2$, $A = u^2Z_1Z_2 - v^3 - 2v^2X_1Z_2$.

倍点公式为

$$X_3 = 2hs, \quad Y_3 = w(4B - h) - 8Y_1^2s^2, \quad Z_3 = 8s^3,$$

其中 $w = aZ_1^2 + 3X_1^2$, $s = Y_1Z_1$, $B = X_1Y_1s, h = w^2 - 8B$.

可见在射影坐标之下, 加法运算和倍点运算所需计算量分别为 $12M + 2S$ 和 $7M + 5S$.

最后, 考虑在 Jacobi 坐标下所需计算量, 令 $P = (X_1, Y_1, Z_1), Q = (X_2, Y_2, Z_2)$ 及 $P + Q = (X_3, Y_3, Z_3)$, 当 $P \neq \pm Q$ 时, 容易推得其加法公式为

$$X_3 = -H^3 - 2U_1H^2 + r^2, \quad Y_3 = -S_1H^3 + r(U_1H^2 - X_3), \quad Z_3 = Z_1Z_2H,$$

其中 $U_1 = X_1Z_2^2$, $U_2 = X_2Z_1^2$, $S_1 = Y_1Z_2^3$, $S_2 = Y_2Z_1^3$, $H = U_2 - U_1$, $r = S_2 - S_1$.

倍点公式为

$$X_3 = T, \quad Y_3 = -8Y_1^4 + M(S - T), \ Z_3 = 2Y_1Z_1,$$

其中 $S = 4X_1Y_1^2$, $M = 3X_1^2 + aZ_1^4$, $T = -2S + M^2$.

在 Jacobi 坐标之下, 加法运算和倍点运算所需计算量分别为 $12M+4S$ 和 $4M+6S$. 可见利用 Jacobi 坐标进行倍点运算速度较快. 还可以有其他一些坐标, 也可以考虑把几种坐标混合使用, 以求达到最好的效果 (参阅文献 [23] 和本书第十九章).

现在考虑如何计算 kP. 最一般的算法, 是取 k 的二进制表示 $k = \sum_{j=0}^{l-1} k_j 2^j$, $k_j \in \{0, 1\}$. 依次做倍点计算 $2P, 4P, \cdots, 2^{l-1}P$, 然后将对应 $k_j = 1$ 的那些项相加. 设 k_j $(0 \leqslant j \leqslant l-1)$ 中有 w 个 1, 则该方法需做 $l-1$ 次倍点运算, $w-1$ 次加法运算. w 的平均值为 $l/2$.

设 $P = (x, y)$, 则 $-P = (x, -y)$, 这是一个可以利用的简单运算, 将 k 表示为 $\sum_{j=0}^{l-1} s_j 2^j$, $s_j \in \{-1, 0, 1\}$, 称它为 (二进制) 带符号表示, s_j $(0 \leqslant j \leqslant l-1)$ 总共有 3^{l+1} 个可能组合, 所表示的 k 可从 $-(2^{l+1} - 1)$ 增至 $2^{l+1} - 1$, 可见一个固定的 k 可以有不同的带符号表示, 例如 $3 = 1 + 2 = -1 + 4$. 为了减少 kP 的计算量, 我们希望选取非零 s_j 个数最少的表示. 当一个带符号表示中任意两个相邻的 s_j 和 s_{j+1} 中至少有一个为零时, 即对任一 $0 \leqslant j \leqslant l-1$ 都有 $s_js_{j+1} = 0$ 时, 称该表示为无关联形式 (NAF). 可以证明 [24] 任一整数都有惟一的 NAF, 且其长度最多比它的最短带符号表示大 1. NAF 中非零系数的平均值为 $l/3$. 可见利用 NAF 可以减少 kP 的计算量.

关于计算 kP 的其他一些方法, 可参阅文献 [7] 的第四章和本书第十九章.

§15.2 小步–大步法

设 P 为椭圆曲线 E 上的点, P 的阶为 n, 已知点 $D \in \langle P \rangle$(P 生成的循环群), 求正整数 l, 使得 $D = lP$ $(0 \leqslant l < n)$.

将 l 表示为

$$l = c\lceil \sqrt{n} \rceil + d, \qquad 0 \leqslant c, d < \lceil \sqrt{n} \rceil,$$

这里 $\lceil \sqrt{n} \rceil$ 表示不小于 $\sqrt{n}$ 的最小正整数. 令 $R_d = D - dP$, 存储关于 R_d $(1 \leqslant d < \lceil \sqrt{n} \rceil)$ 的表, 对于 $c = 0, 1, \cdots, \lceil \sqrt{n} \rceil - 1$, 依次计算 $S_c = c\lceil \sqrt{n} \rceil P$. 将 S_c 与 R_d 表中的点比较, 若某个 S_{c_0} 与 R_{d_0} 相同, 则有 $l = c_0\lceil \sqrt{n} \rceil + d_0$.

计算 R_d 可叫做小步, 计算 S_c 可叫做大步, 文献上将这个方法称为 “小步 – 大步” 方法. 它要求存储 R_d 表, 存储量为 $O(\sqrt{n})$ 个 E 的点. 小步和大步都要求 $O(\sqrt{n})$ 次 E 上点的运算, 所以该方法的计算复杂度为 $O(\sqrt{n})$. 这是迄今为止所知道的计算任意椭圆曲线的 ECDLP 最好的复杂度.

下节将介绍 Pollard 的方法 [26], 它们也可用于计算任意椭圆曲线的 ECDLP, 计算复杂度也是 $O(\sqrt{n})$, 但仅需要很小的存储量. 这里先介绍 Pohlig 和 Hellman[27] 处理 ECDLP 的一个方法, 它指出仅需考虑 P 的阶 n 为素数时的 ECDLP.

设 $n = \prod p_i^{c_i}$ 为标准因子分解, p_i 为素数. 若对每个 $p_i^{c_i}$ 能计算 $l \mod p_i^{c_i}$, 则由中国剩余定理就可得到 l. 令 $n_i = n/p_i^{c_i}$, 则

$$D_i = n_i D = l(n_i P) = lP_i,$$

P_i 的阶为 $p_i^{c_i}$, 因而对每个 i, 计算 n 为 $p_i^{c_i}$ 的 ECDLP 就可得到 $l \mod p_i^{c_i}$.

进一步, 设 $n = p^c$ 为素数幂, 令

$$D_0 = p^{c-1}D = l(p^{c-1}P) = lP_0,$$

P_0 的阶为 p, 计算该 $n = p$ 的 ECDLP 可得到 $l \equiv l_0 \mod p$ $(0 \leqslant l_0 < p)$. 设 $l = l_0 + l_1 p$, 则

$$D_1' = D - l_0 P = l_1(pP) = l_1 P_1',$$

P_1 的阶为 p^{c-1}. 类似地, 令

$$D_1 = p^{c-2}D_1' = l_1(p^{c-2}P_1') = l_1 P_1,$$

P_1 的阶为 p, 计算该 ECDLP 可得到 $l_1 \mod p$, 从而得到 $l \mod p^2$. 重复使用上述方法, 可依次得到 $l \mod p^i$ $(i = 1, 2, \cdots, c)$.

由于存在 Pohlig 和 Hellman 的方法, 我们在使用椭圆曲线公钥密码时, 要求选取基点 P 的阶 n 是一个大素数, 使得 $O(\sqrt{n})$ 的计算量不能实现. 因而在选取椭圆曲线时, 要求它的阶 (其上点的个数) 是一个大素数或是一个近似素数 (一个大素数与几个小素因子之积), 本书的第二部分和第三部分已经详细讨论了如何构造这样的椭圆曲线.

本节所讨论的方法适用于任意交换群上的离散对数的计算.

§15.3 家袋鼠和野袋鼠

袋鼠的跳跃看似一随机的游动, 事实上并非如此, 它每次跳跃的方向和距离都由起跳点的状态所决定. 设想在一块地里, 1 只家袋鼠带 1 把铲子, 它每跳 10 步就在所到达的地方挖一个洞, 并把洞口伪装起来. 之后如果一只野袋鼠进入同一块地里, 只要它一旦碰到家袋鼠的足迹, 则它最多跳 10 步就会掉入一个洞中. 这个家袋鼠逮野袋鼠的方法, 可用于计算离散对数.

设 G 为 n 阶有限交换群, $P, D \in G$ 且 $D = mP$, 我们要计算 m. 定义函数

$$f: \quad G \longrightarrow \{1, 2, \cdots, s\},$$

s 是一个可以选择的正整数. 假设 f 是一致分布的, 即

$$\sum_{i=1}^{s} \left| \#\{g \in G | f(g) = i\} - \frac{n}{s} \right| = O(\sqrt{n}).$$

令

$$M_i = a_i P + b_i D, \qquad a_i, b_i \in \mathbb{Z}, \quad i = 1, 2, \cdots, s,$$

定义函数

$$\begin{aligned} F: \ G &\longrightarrow G \\ g &\longmapsto g + M_{f(g)}, \end{aligned}$$

从 g_0 出发, 通过 $g_k = F(g_{k-1})$ 就可得到一个随机游动.

上述家袋鼠逮野袋鼠的方法即为: 在 G 中取两点

$$g_0 = x_0 P + x_0' D, \qquad h_0 = y_0 P + y_0' D.$$

利用以上通过 F 定义的游动计算

$$g_k = x_k P + x_k' D, \quad h_k = y_k P + y_k' D, \qquad k = 1, 2, \cdots,$$

如果能找到 i 和 l, 使得 $g_i = h_l$, 则有 $x_iP + x_i'D = y_lP + y_l'D$, 从而 $(x_i' - y_l')D = (y_l - x_i)P$, 当 $x_i' - y_l'$ 与 n 互素时, 即可得到 m. 事实上, 在计算过程中若出现某两个 g_k 相同, 或某两个 h_k 相同, 也有可能得到离散对数 m.

粗略地估计一下该方法所需要的计算量, 计算 g_0, h_0 后, $g_0 \neq h_0$ 的概率为$1 - \frac{1}{n}$, 计算 g_1 后, $g_1 \neq g_0, h_0$ 的概率为 $1 - \frac{2}{n}$, 计算 h_1 后, $h_1 \neq g_0, g_1, h_0$ 的概率为 $1 - \frac{3}{n}$, 依次类推, 在计算 $g_0, \cdots, g_{k-1}, h_0, \cdots, h_{k-1}$ 后, 其中不出现两个相同的元素的概率为

$$\left(1 - \frac{1}{n}\right)\left(1 - \frac{2}{n}\right) \cdots \left(1 - \frac{2k}{n}\right) \sim 1 - \frac{1}{n}\sum_{i=1}^{2k} i$$

(当 n 很大时), 因而出现两个相同元素的概率约为 $k(2k-1)/n$, 可见所需计算量为 $O(\sqrt{n})$.

为了发现 $\{g_k\}$ 与 $\{h_k\}$ 之间的碰撞, 可将所计算的 g_k 和 h_k 都存储起来, 但这样所需的存储量较大. 为了减少存储量, 定义 G 上的一个函数 $H: G \longrightarrow \mathbb{Z}$, 当 $H(g)$ 具有某种性质时, 譬如它的二进制表达式中最底的 i 位都为零时, 称 g 为判别元. 我们仅存储 g_k 和 h_k 中的判别元, 寻找判别元之间的碰撞, 这时存储量为原来的 $1/2^i$, 但计算量将平均增加 2^i 倍, 在将该方法用于 ECDLP 时, 可以取 g 的 x 坐标作为 $H(g)$.

§15.4　MOV 约化

这是 Menezes, Okamoto 和 Vanstone 提出的一个计算 ECDLP 的方法 [28], 设 $E/\mathbb{F}_q$ 为椭圆曲线, 点 $P \in E(\mathbb{F}_q)$ 的阶为 n, 假设 n 与 q 互素 (这是应用中最常见的情形), 已知 $D \in \langle P \rangle$ 计算 l, 使得 $D = lP$.

假设 k 为最小正整数, 使得 $E[n] \subset E(\mathbb{F}_{q^k})$, 因而 $\mathbb{F}_{q^k}$ 中包含 n 次单位根 μ_n.

引理 15.1　*设 $P_1, P_2 \in E[n]$, 则 $e_n(P, P_1) = e_n(P, P_2)$ 的充分必要条件是 P_1 和 P_2 属于 $\langle P \rangle$ 在 $E[n]$ 中的同一陪集.*

证明　若 P_1 与 P_2 属于 $\langle P \rangle$ 的同一陪集, 则存在正整数 k, 使得 $P_1 = P_2 + kP$, 则

$$e_n(P, P_1) = e_n(P, P_2 + kP) = e_n(P, P_2)e_n(P, P)^k = e_n(P, P_2).$$

若 P_1 与 P_2 属于不同的陪集, 因 $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$, 可找到 $Q \in E[n]$, 使得 Q 和 P 为 $E[n]$ 的一组基, 因而 $P_1 - P_2 = a_1P + a_2Q$, 且 $a_2Q \neq \mathcal{O}$. 设 $b_1P + b_2Q$ 为 $E[n]$ 的任一点, 则

$$e_n(a_2Q, b_1P + b_2Q) = e_n(a_2Q, P)^{b_1}e_2(Q, Q)^{a_2b_2} = e_n(a_2Q, P)^{b_1},$$

可见 $e_n(a_2Q,P)\neq 1$, 否则将有 $a_2Q=\mathcal{O}$, 从而

$$e_n(P,P_1)e_n(P,P_2)^{-1}=e_n(P,a_1P+a_2Q)=e_n(P,a_2Q)\neq 1.$$

证毕.

定理 15.1 设 $P\in E[n]$, 一定存在 $Q\in E[n]$, 使得 $e_n(P,Q)$ 为 n 次本原单位根.

证明 $\langle P\rangle$ 在 $E[n]$ 中有 n 个不同的陪集, 对任一 $Q\in E[n]$, $e_n(P,Q)$ 为 n 次单位根, 由引理 15.1, 当 Q 跑遍 n 个不同的陪集时, $e_n(P,Q)$ 跑遍所有的 n 次单位根, 证毕.

设 $\alpha=e_n(P,Q)\in\mathbb{F}_{q^k}$ 为 n 次本原单位根, 记 $\beta=e_n(D,Q)\in\mathbb{F}_{q^k}$. 若在 $\mathbb{F}_{q^k}$ 中能计算以 α 为基 β 的离散对数 l, 即 $\beta=\alpha^l$, 则

$$e_n(D,Q)=e_n(P,Q)^l=e_n(lP,Q),$$

令 $D-lP=sP$, 从而

$$e_n(P,Q)^s=e_n(sP,Q)=e_n(D,Q)\cdot e_n(P,Q)^{-l}=1,$$

由于 $e_n(P,Q)$ 为 n 次本原单位根, 可见 $n|s, D=lP$.

上述方法将椭圆曲线上的离散对数的计算归结为有限域 $\mathbb{F}_{q^k}$ 上离散对数的计算, 这个约化过程包括以下两个步骤:

(1) 找到最小的正整数 k, 使得 $E[n]\subset E(\mathbb{F}_{q^k})$;
(2) 找到点 $Q\in E[n]$, 使得 $e_n(P,Q)$ 为 n 次本原单位根. (15.1)

可以利用 §3.4 中的方法计算 Weil 对: 关于 $f_T(D_S)$ 的计算, §3.4 中的推导过程实际上给出了计算函数 f_T, 使得 $\mathrm{div}(f_T)=n(T)-n(\mathcal{O})$ 的方法, 但在这里并不一定要计算函数 f_T, 而是要计算它在某些点的值. 假设要计算 $f_T(S)$, 定义 $\langle T\rangle\times\mathbb{F}_q^*$ 上的一个群运算

$$(r_1T,a_1)\oplus(r_2T,a_2)=\big((r_1+r_2)T,a_1a_2h(S)\big),$$

其中

$$\mathrm{div}(h)=(r_1T)+(r_2T)-\big((r_1+r_2)T\big)-(\mathcal{O}).$$

设 $n=\alpha_0+2\alpha_1+\cdots+2^s\alpha_s$ $(\alpha_i=0,1)$, 从 $(T,1)$ 出发, 依次计算 $(2T,a_1),(4T,a_2),\cdots,(2^sT,a_s)$(其中 $a_i=f_i(S),\mathrm{div}f_i\sim 2^i(T)-(2^iT)-(2^i-1)(\mathcal{O})$), 然后计算 $\alpha_0(T,1)\oplus\alpha_1(2T,a_1)\oplus\cdots\oplus\alpha_s(2^sT,a_s)=(\mathcal{O},f_T(S))$. 以 $R(n)$ 表示上述计算进程中出现的 iT $(0\leqslant i<n)$ 的集合, 只要 $S\notin R(n)$, 上述计算是可行的. 若计算 $f_T(D_S)$, 只要找到整数 k, 使得 $(k+1)S$ 与 kS 都不在 $R(n)$ 中出现, 取 $D_S=\big((k+1)S\big)-(kS)\sim(S)-(\mathcal{O})$, 则 $f_T(D_S)=f_T\big((k+1)S\big)/f_T(kS)$. 计算 $f_T(S)$ 的计算量为 $O(\log n)$.

下面就一类特殊的椭圆曲线 —— 超奇异椭圆曲线, 讨论如何利用 MOV 约化.

设 $\mathbb{F}_q$ 的特征为 p, 当 $E/\mathbb{F}_q$ 的 q 阶 Frobenius 变换的迹 t 是 p 的倍数时, E 称为超奇异的.

我们有 $|q+1-\#E(\mathbb{F}_q)| \leqslant 2\sqrt{q}$. 反之, 若 $|t| \leqslant 2\sqrt{q}$, 是否存在椭圆曲线 $E/\mathbb{F}_q$, 使得 $\#E(\mathbb{F}_q) = q+1-t$?

定理 15.2 设 $q = p^m$, 当且仅当 t 适合下述条件之一时, 存在椭圆曲线 $E/\mathbb{F}_q$, 使得 $\#E(\mathbb{F}_q) = q+1-t$:

1. $p \nmid t$, $t^2 \leqslant 4q$;

2. m 是奇数, 下列条件之一成立:

(a) $t = 0$;

(b) $t^2 = 2q$, $p = 2$;

(c) $t^2 = 3q$, $p = 3$;

3. m 是偶数, 下列条件之一成立:

(a) $t^2 = 4q$;

(b) $t^2 = q$, $p \not\equiv 1 \mod 3$;

(c) $t = 0$, $p \not\equiv 1 \mod 4$.

证明见文献 [29].

由定理 15.2 可知, 当且仅当 $t^2 = 0, q, 2q, 3q, 4q$ 时, E 为超奇异椭圆曲线.

设 K 为 $\mathbb{Q}$ 上的 2 次虚域, $O_{\max}$ 表示 K 中的代数整数环, 1 和 ω 为它在 $\mathbb{Z}$ 上的一组基. $O_{\max}$ 中任一形如 $O = \mathbb{Z} + k\omega\mathbb{Z}$($k$ 为任一正整数) 的子环, 称为序 (order), O 的判别式 $\Delta(O) = \Delta(O_{\max})k^2$, 所以 O 也由它的判别式惟一决定, 以 $O(\Delta)$ 表示判别式为 Δ 的序.

定理 15.3 $\mathbb{F}_q$ 的特征为 p, 正整数 n 与 p 互素, $E/\mathbb{F}_q$ 上的 q 阶 Frobenius 变换 ϕ 的迹为 t, 则下述条件等价:

(1) $E[n] \subset E(\mathbb{F}_q)$;

(2) $n^2 |\, q+1-t$, $n | q-1$, $\phi \in \mathbb{Z}$ 或 $O(\frac{t^2-4q}{n}) \subset \mathrm{End}_{\mathbb{F}_q}(E)$.

其中 $\mathrm{End}_{\mathbb{F}_q}(E)$ 是定义在 $\mathbb{F}_q$ 上的 E 的同种映射组成的环.

证明 因 $\mathrm{Ker}(\phi-1) = E(\mathbb{F}_q)$, $\mathrm{Ker}([n]) = E[n]$, 条件 (1) 成立的充分必要条件为

$$\frac{\phi-1}{n} \in \mathrm{End}_{\mathbb{F}_q}(E). \tag{15.2}$$

若 $\phi \in \mathbb{Z}$, 条件 (15.2) 等价于 $n|\phi-1$. 这时 $q = \phi\widehat{\phi} = \phi^2$, $t = \phi + \widehat{\phi} = 2\phi$, 因而 $q+1-t = (\phi-1)^2$, 所以 $n|\phi-1$ 等价于 $n^2|q+1-t$. 因 $q-1 = \phi^2-1$, 条件 $n|q-1$ 自然也成立.

若 $\phi \notin \mathbb{Z}$. 这时 $\mathbb{Q}(\phi) \subset \mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Q} \subset \mathrm{End}(E) \otimes \mathbb{Q}$, $\mathbb{Q}(\alpha)$ 是 $\mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Q}$ 的中心, $\mathbb{Q}(\alpha)$ 是 2 次虚域, 故 $\mathrm{End}_{\mathbb{F}_q}(E) \otimes \mathbb{Q} = \mathbb{Q}(\alpha)$, 所以 $\mathrm{End}_{\mathbb{F}_q}(E)$ 是 $\mathbb{Q}(\alpha)$ 中的一个序. 条件 (15.2) 等价于: $\frac{\phi-1}{n}$ 是 $\mathrm{End}_{\mathbb{F}_q}(E)$ 中的代数整数. 计算 $\frac{\phi-1}{n}$ 的范数、迹和 $\mathbb{Z}[\frac{\phi-1}{n}]$ 的判别式

$$\begin{aligned} N\Big(\frac{\phi-1}{n}\Big) &= \frac{\phi-1}{n} \cdot \frac{\widehat{\phi}-1}{n} = \frac{q+1-t}{n^2}, \\ T\Big(\frac{\phi-1}{n}\Big) &= \frac{\phi-1}{n} + \frac{\widehat{\phi}-1}{n} = \frac{t-2}{n} = \frac{q-1}{n} - \frac{q+1-t}{n}, \\ \Delta\Big(\mathbb{Z}\Big[\frac{\phi-1}{n}\Big]\Big) &= T\Big(\frac{\phi-1}{n}^2\Big) - 4N\Big(\frac{\phi-1}{n}\Big) = \frac{t^2-4q}{n^2}, \end{aligned}$$

可见条件 (1) 与 (2) 等价, 证毕.

定理 15.4 $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, 且 $n_2|n_1$, $n_2|q-1$.

证明 设 m 为 $E(\mathbb{F}_q)$ 中各点的阶的最小公倍数. 首先假设 m 与 q 互素, 一定存在 $\mathbb{F}_q$ 的某一扩域 $\mathbb{F}_{q^k}$, 使得 $E[m] \subset E(\mathbb{F}_{q^k})$, $E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$. $E(\mathbb{F}_q)$ 是 $E[m]$ 的子群, 故 $E(\mathbb{F}_q) \cong \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2}$, 利用交换群基本定理, 可得 $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, $n_2|n_1$. 这时由于 $E[n_2] \subset E(\mathbb{F}_q)$, 故有 $n_2|q-1$(定理 15.3). 当 m 与 q 不互素时, 则有 $m = p^r \cdot m'$, m' 与 q 互素, 素数 $p|q$. 这时 $E(\mathbb{F}_q) \cong \mathbb{Z}_{p^r} \oplus E(\mathbb{F}_q)'$, $E(\mathbb{F}_q)'$ 各元素的阶的最小公倍数即为 m', 它与 q 互素, 对 $E(\mathbb{F}_q)'$ 应用上述已证的结果得到 $E(\mathbb{F}_q)' \cong \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2}$, 因而 $E(\mathbb{F}_q) \cong \mathbb{Z}_{p^r n_1} \oplus \mathbb{Z}_{n_2}$, 证毕.

下面的定理 15.5 给出了当 $E/\mathbb{F}_q$ 为超奇异椭圆曲线时 $E(\mathbb{F}_q)$ 的群结构.

定理 15.5 *设 $t \in \mathbb{Z}$ 为 $E/\mathbb{F}_q$ 上的 q 阶 Frobenius 变换 ϕ 的迹, $E/\mathbb{F}_q$ 为超奇异.*

1. 若 $t^2 = q,\ 2q,$ 或$3q$, 则 $E(\mathbb{F}_q)$ 为循环群;

2. 若 $t^2 = 4q$, 当 $t = 2\sqrt{q}$ 时, $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}-1} \oplus \mathbb{Z}_{\sqrt{q}-1}$; 当 $t = -2\sqrt{q}$ 时, $E(\mathbb{F}_q) \cong \mathbb{Z}_{\sqrt{q}+1} \oplus \mathbb{Z}_{\sqrt{q}+1}$;

3. 若 $t = 0$, $q \not\equiv -1 \mod 4$, 则 $E(\mathbb{F}_q)$ 为循环群; 若 $t = 0$, $q \equiv -1 \mod 4$, 则 $E(\mathbb{F}_q)$ 为循环群或 $E(\mathbb{F}_q) \cong \mathbb{Z}_{(q+1)/2} \oplus \mathbb{Z}_2$.

证明 记 $t^2 = \alpha q$, $\alpha = 0,1,2,3,4$. 假设 $E[m] \subset E(\mathbb{F}_q)$, 且 $E[m] \cong \mathbb{Z}_m \oplus \mathbb{Z}_m$. 这时 m 与 q 互素, 因而 $m^2|q+1-t$, $m|q-1$, 由此得到 $q \equiv 1 \pmod m$, $t \equiv 2 \pmod m$. 由于 $(t-2)^2 = \alpha q - 4t + 4 \equiv \alpha - 4 \pmod m$, 故 $m|4-\alpha$.

若 $\alpha = 3$, 由于 $m|1$, 一定有 $m = 1$; 若 $\alpha = 2$, 这时 $m|2$ 且 m 与 2 互素, 故只能有 $m = 1$; 若 $\alpha = 1$, 这时 $m|3$, 由于 $q+1 \pm \sqrt{q}$ 一定不是 9 的倍数, 所以 $m \neq 3$, 同样只能有 $m = 1$, (1) 成立.

若 $\alpha = 4$, 当 $t = 2\sqrt{q}$ 时, ϕ 适合 $x^2 - 2\sqrt{q} + q = 0$, 所以 $\phi = \sqrt{q} \in \mathbb{Z}$. 取

$m=\sqrt{q}-1$, 这时定理 15.3 的 (2) 成立, 由于 $\#E(\mathbb{F}_q)=q+1-2\sqrt{q}=(\sqrt{q}-1)^2$, 所以 $E(\mathbb{F}_q)\cong\mathbb{Z}_{\sqrt{q}-1}\oplus\mathbb{Z}_{\sqrt{q}-1}$. 类似地可以证明当 $t=-2\sqrt{q}$ 时, $E(\mathbb{F}_q)\cong\mathbb{Z}_{\sqrt{q}+1}\oplus\mathbb{Z}_{\sqrt{q}+1}$, (2) 成立.

若 $\alpha=0$, 这时 $m|4$, m 可能为 $1,2,4$. 当 $q\not\equiv-1\mod 4$ 时, 由于 $m^2|q+1$, 可知 m 只能为 1; 当 $q\equiv-1\mod 4$ 时, 由于 $m|q-1$, 可知 m 为 1 或 2, 于是 (3) 成立, 证毕.

设 $E/\mathbb{F}_q$ 为超奇异椭圆曲线, $E(\mathbb{F}_q)=\mathbb{Z}_{n_1}\oplus\mathbb{Z}_{n_2}$, $n_2|n_1$, n_1 和 n_2 由定理 15.5 所决定. 要完成 (15.1) 中的步骤 (1), 实际上就是要找到最小的正整数 k, 使得 $E[n_1]\subset E(F_{q^k})$, 因为 n 是 n_1 的因子, 这时自然有 $E[n]\subset E(F_{q^k})$. 依 $t^2=0,q,2q,3q,4q$ 的不同情形分别讨论. 当 $t^2=4q$ 时, 根据定理 15.5 的 (2), 显然有 $k=1$. 当 $t^2=q$ 时, $n_1=q+1\mp\sqrt{q}$, 因 $q^3-1=(q-1)(q+1+\sqrt{q})(q+1-\sqrt{q})$, 所以 $n_1|q^3-1$. $E/\mathbb{F}_{q^3}$ 上的 q^3 阶 Frobenius 变换 ϕ_{q^3} 适合方程 $x^2\pm2\sqrt{q^3}x+q^3=0$(利用 3.23 式得 $V_3=\mp2\sqrt{q^3}$), 因而 $\phi_{p^3}=\pm\sqrt{q^3}\in\mathbb{Z}$. 由于 $q^3+1\pm2\sqrt{q^3}=(\sqrt{q}\pm1)^2(q+1\mp\sqrt{q})^2$, 可见 $n_1^2|q^3+1\pm2\sqrt{q^3}$, 所以 $E[n_1]\subset E(\mathbb{F}_{q^3})$(定理 15.3(2)), 可取 $k=3$. 利用类似方法, 当 $t^2=2q$ 时, 可取 $k=4$; 当 $t^2=3q$ 时, 可取 $k=6$; 当 $t^2=0$ 时, 可取 $k=2$. 在上述所有情形下都有 $E(\mathbb{F}_{q^k})\cong\mathbb{Z}_{cn_1}\oplus\mathbb{Z}_{cn_1}$, 其中 c 为正整数.

(15.1) 中的约化步骤 (2) 可如下进行：任取 $Q'\in E(\mathbb{F}_{q^k})$, 令 $Q=(cn_1/n)Q'$ ($\in E[n]$). 计算 $\alpha=e_n(P,Q)$, $\beta=e_n(D,Q)$, 在 F_{q^k} 中计算离散对数 l', 使得 $\beta=\alpha^{l'}$. 若 $D=l'P$, 则计算完成. 否则, 说明 α 不是 n 次本原单位根, 改取另一 Q', 重复上述过程, 直到找到 l 使 $D=lP$. 找到 Q 使 α 为 n 次本原单位根的概率为 $\phi(n)/n$(ϕ 为欧拉函数).

一个概率型算法, 如果它的计算时间的期望值以输入变量 x 的比特长度 (即 $\log x$) 的多项式为上界, 则称它为概率多项式算法. 如果该期望值以函数

$$L(\alpha,x)=\exp((c+o(1))(\log x)^{\alpha}(\log\log x)^{1-\alpha}),\ 0<\alpha<1$$

为上界, 则称为概率亚指数算法, 这里 $o(1)$ 表示无穷小量.

假设已有 $\mathbb{F}_q$ 在其素域 $\mathbb{F}_p$ 上的一组基, 随机取 $\mathbb{F}_q[x]$ 中一 k 次不可约多项式 $f(x)$, 这是一个概率多项式算法 ($\log q$ 的多项式), 于是得到 $\mathbb{F}_{q^k}\cong\mathbb{F}_q[x]/(f(x))$. 当 $k\leqslant6$ 时, 随机取 $Q'\in E(\mathbb{F}_{q^k})$ 是一个概率多项式算法, 由 Q' 确定 Q 是多项式算法. 计算 Weil 对是多项式算法, 由于

$$n/\phi(n)\leqslant b\log\log n,\quad n\geqslant5$$

以及 $n=O(q)$, 通过 $O(\log\log q)$ 次迭代可以找到 Q, 使得 $e_n(P,Q)$ 为 n 次本原单位根. 检查 $D=l'P$ 是否成立是多项式算法. 综合上述, 将超奇异椭圆曲线上的 ECDLP 化为 $\mathbb{F}_{q^k}$ 上的 DLP 是概率多项式算法. 关于有限域上的离散对数计算, 当

p 固定, $p \to \infty$ 时, 已有计算 $\mathbb{F}_{q^k}$ 上的离散对数的概率亚指数算法 (见 §15.7). 综合上述, 对于超奇异椭圆曲线上的 ECDLP 有概率亚指数算法. 我们在构造椭圆曲线公钥密码时, 将不采用超奇异椭圆曲线.

§15.5 FR 约化

Frey, Müller 和 Rück[30] 利用 Tate 对给出一个方法, 在一定条件下 $(n|q-1)$, 将 $\mathbb{F}_q$ 上的曲线的除子类群中的离散对数的计算化为 $\mathbb{F}_q^*$ 中离散对数的计算. 由于椭圆曲线与除子类群 $\mathrm{Pic}^\circ(E)$ 是同构的, 本节将 FR 约化应用于椭圆曲线[31].

首先, 简单介绍群的上同调.

设 G 为有限群, M 为交换群, G 中元素可作用在 M 上. 将 $\delta \in G$ 在 $m \in M$ 上的作用记为 $m \mapsto m^\delta$, 并假定它满足条件

$$m^1 = m, \qquad (m+m')^\delta = m^\delta + m'^\delta, \qquad (m^\delta)^\tau = m^{\delta\tau},$$

其中 1 为 G 的单位, 这时称 M 为 G 模. 设 M 和 N 为两个 G 模, $\phi:\ M \longrightarrow N$ 为同态, 且适合

$$\phi(m)^\delta = \phi(m^\delta), \qquad \forall m \in M,\ \delta \in G,$$

称 ϕ 为 G 同态.

定义 15.1 *G 模 M 的零阶上同调群为*

$$H^\circ(G,M) = \{m \in M:\ \ m = m^\delta,\ \forall \delta \in G\},$$

即 $H^\circ(G,M)$ 为 M 中由 G 不变元素组成的子模, 有时也记作 M^G.

设

$$0 \longrightarrow P \xrightarrow{\phi} M \xrightarrow{\psi} N \longrightarrow 0$$

是 G 模正合序列 (即序列中前一 G 同态的像是后一 G 同态的核), 可见 ϕ 是单射, ψ 是满射, 且 ϕ 的像为 ψ 的核. 在每个 G 模中取 G 不变量, 得到 G 模正合序列

$$0 \longrightarrow P^G \xrightarrow{\phi} M^G \xrightarrow{\psi} N^G$$

最右端的 G 同态就不一定是映上的, 为了研究它的像集, 引入下述定义:

定义 15.2 *设 M 为 G 模, 令*

$$C^1(G,M) = \{\ \xi:\ \ G \longrightarrow M\ \}$$

为由 G 到 M 的所有映射 (也称 1 链) 组成的 (加法) 群, 令

$$Z^1(G,M) = \{\ \xi \in C^1(G,M):\ \ \xi_{\delta\tau} = \xi_\delta^\tau + \xi_\tau,\ \forall \delta,\tau \in G\ \}$$

为由 G 到 M 的 1 闭上链组成的群, 令

$$\mathcal{B}^1(G,M)=\{\ \xi\in C^1(G,M):\ 存在 m\in M, 使得\ \xi_\delta=m^\delta-m,\ \forall\delta\in G\ \}$$

为由 G 到 M 的 1 上边缘组成的群. 显然 $\mathcal{B}^1(G,M)\subset Z^1(G,M)$. G 模 M 的1阶上同调群 $H^1(G,M)$ 定义为

$$H^1(G,M)=Z^1(G,M)/\mathcal{B}^1(G,M),$$

两个 1 闭上链之差若为 1 上边缘, 它们对应 $H^1(G,M)$ 中同一上同调类.

设 ϕ: $M\longrightarrow N$ 为 G 同态, 则 ϕ 将 $Z^1(G,M)$ 中映射到 $Z^1(G,N)$, 将 $\mathcal{B}^1(G,M)$ 映射到 $\mathcal{B}^1(G,N)$, 所以 ϕ 诱导映射 $H^1(G,M)\longrightarrow H^1(G,N)$.

定理 15.6　设

$$0\longrightarrow P\xrightarrow{\phi}M\xrightarrow{\psi}N\longrightarrow 0$$

是 G 模正合序列, 则有正合序列

$$\begin{aligned}0\longrightarrow H^\circ(G,P)\longrightarrow H^\circ(G,M)\longrightarrow H^\circ(G,N)&\\ \xrightarrow{\delta}H^1(G,P)\longrightarrow H^1(G,M)\longrightarrow H^1(G,N),&\end{aligned}$$

其中 δ 定义为: 对任一 $n\in H^\circ(G,N)$, 取 $m\in M$, 使得 $\psi(m)=n$, 定义 1 闭上链 $\xi\in Z^1(G,P)$:

$$\xi_\delta=m^\delta-m,\quad\forall\delta\in G,$$

$\delta(n)$ 即为 ξ 在 $H^1(G,P)$ 中所属的上同调类.

证明　因 $n\in N^G$, 故 $\psi(\xi_\delta)=\psi(m)^\delta-\psi(m)=n^\delta-n=0$, 所以 $\xi_\delta\in\mathrm{Ker}\psi=\mathrm{Im}(\phi)\cong P$, 可以认为 ξ_δ 属于 P, 即 $\xi\in H^1(G,P)$. 易见 ξ 所在的上同调类不依赖于 m 的选择. 证明的其余部分虽然比较繁琐, 但都是可以根据定义直接推出的, 证毕.

将定理 15.6 应用于椭圆曲线, 设 $E'/\mathbb{F}_q$ 和 $E/\mathbb{F}_q$ 为椭圆曲线, ϕ 为定义在 $\mathbb{F}_q$ 上的同种映射 $E'\longrightarrow E$. 取 $G=\mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$, 有 G 模正合序列

$$0\longrightarrow E'[\phi]\longrightarrow E'(\overline{\mathbb{F}}_q)\xrightarrow{\phi}E(\overline{\mathbb{F}}_q)\longrightarrow 0,$$

$E'[\phi]$ 表示 ϕ 的核. 利用定理 15.6, 得到正合序列

$$0\longrightarrow E'(\mathbb{F}_q)[\phi]\longrightarrow E'(\mathbb{F}_q)\xrightarrow{\phi}E(\mathbb{F}_q)\xrightarrow{\delta_E}H^1(G,E'[\phi])\longrightarrow H^1(G,E'(\overline{\mathbb{F}}_q)),$$

可见有正合序列

$$0\longrightarrow E(\mathbb{F}_q)/\phi(E'(\mathbb{F}_q))\xrightarrow{\delta_E}H^1(G,E'[\phi])\xrightarrow{\phi}H^1(G,E'(\overline{\mathbb{F}}_q))[\phi]\longrightarrow 0,$$

其中

$$\begin{array}{rccc} \delta_E: & E(\mathbb{F}_q)/\phi(E'(\mathbb{F}_q)) & \longrightarrow & H^1(G,E'[\phi]) \\ & P & \longmapsto & \delta\mapsto Q^\delta - Q, \end{array}$$

这里 $P\in E(\mathbb{F}_q)$, $Q\in E'(\overline{\mathbb{F}}_q)$, $\phi(Q)=P$.

设 n 为正整数, n 与 q 互素, 考虑乘法群 $\overline{\mathbb{F}}_q^*$ 中 n 次幂运算, 得 G 模正合序列

$$1\longrightarrow \mu_n \longrightarrow \overline{\mathbb{F}}_q^* \longrightarrow \overline{\mathbb{F}}_q^* \longrightarrow 1.$$

假设 $\mu_n\subset\mathbb{F}_q$, 即 $n|q-1$, 利用定理 15.6 可得到正合序列

$$1\longrightarrow \mu_n \longrightarrow \mathbb{F}_q^* \xrightarrow{n} \mathbb{F}_q^* \xrightarrow{\delta_F} H^1(G,\mu_n) \longrightarrow H^1(G,\overline{\mathbb{F}}_q^*),$$

由于 $H^1(G,\overline{\mathbb{F}}_q^*)=1$ (Hilbert 定理 90), 可得正合序列

$$1\longrightarrow \mathbb{F}_q^*/(\mathbb{F}_q^*)^n \xrightarrow{\delta_E} H^1(G,\mu_n) \longrightarrow 1,$$

其中

$$\begin{array}{rccc} \delta_F: & \mathbb{F}_q^*/(\mathbb{F}_q^*)^n & \longrightarrow & H^1(G,\mu_n) \\ & b & \longmapsto & \delta\mapsto \beta^\delta/\beta \end{array}$$

是一个同构, 这里 $\beta\in\overline{\mathbb{F}}_q^*$, 且 $\beta^n=b$.

特别地, 取 $E'=E$, $\phi=[n]$, 利用 Weil 对 e_n: $E[n]\times E[n]\longrightarrow\mu_n$ 定义 Tate 对

$$\begin{array}{rccc} b: & E(\mathbb{F}_q)/n(E(\mathbb{F}_q))\times E(\mathbb{F}_q)[n] & \longrightarrow & \mathbb{F}_q^*/(\mathbb{F}_q^*)^n \\ & (P,T) & \longmapsto & \delta_F^{-1}\big(e_n(\delta_E(P),T)\big), \end{array}$$

这里 $e_n(\delta_E(P),T)\in H^1(G,\mu_n)$, $e_n(\delta_E(P)(\delta),T)=\beta^\delta/\beta$ ($\forall\ \delta\in G$), 其中 $\beta^n=b(P,T)$.

由 Weil 对的双线性, 不难推出 $b(P,T)$ 的双线性. 可以证明 $b(P,T)$ 是非退化的 [32]. $b(P,T)$ 可用以下的方法计算: 由于 $T\in E(\mathbb{F}_q)[n]$, 可找到函数 f_T, $g_T\in\mathbb{F}_q(E)$, 使得

$$\operatorname{div}(f_T)=n(T)-n(\mathcal{O}),\quad f_T\circ[n]=g_T^n,$$

因而

$$e_n(\delta_E(P)(\delta),T)=e_n(Q^\delta-Q,T)=g_T(X+Q^\delta-Q)/g_T(X),$$

取 $X=Q$, 由于 $g_T\in\mathbb{F}_q(E)$, 故得

$$g_T(Q^\delta)/g_T(Q)=g_T(Q)^\delta/g_T(Q),$$

所以当 $P \neq T$ 时,

$$b(P,T) = g_T(Q)^n = f_T \cdot [n](Q) = f_T(P) \pmod{\mathbb{F}_q^{*n}}.$$

当 $P = T$ 时, 任取 $P_1 \in E(\mathbb{F}_q)$, 使得 $P + P_1$, $P_1 \notin R(n)$(定义见 §15.4), 利用 b 的双线性得到

$$b(T,T) \equiv f_T(T + P_1) \cdot f_T(P_1)^{-1} \pmod{\mathbb{F}_q^{*n}}.$$

当 $n|q-1$ 时, 有同构映射

$$\begin{aligned} \gamma:\ \mathbb{F}_q^*/(\mathbb{F}_q^*)^n &\longrightarrow \mu_n \\ a &\longmapsto a^{\frac{q-1}{n}}. \end{aligned}$$

将 b 与 γ 复合, 得到 Tate-Lichtenbaum 对

$$\begin{aligned} \Phi_m:\ E(\mathbb{F}_q)/n(E(\mathbb{F}_q)) \times E(\mathbb{F}_q)[n] &\longrightarrow \mu_n \\ (P,T) &\longmapsto \big(b(P,T)\big)^{\frac{q-1}{n}}. \end{aligned}$$

注 15.1　f_T 的选取可以相差一个常数因子, 但由于 $f_T \cdot [n] = g_T^n$, 故该常数因子属于 $\mathbb{F}_q^{*n}$, 即在 mod $\mathbb{F}_q^{*n}$ 的意义下, f_T 是惟一的.

注 15.2　对于 Weil 对, 一定有 $e_n(T,T) = 1$. 但对于 Tate-Lichtenbaum 对, $\Phi_m(T,T)$ 不一定是 1, 它将在离散对数的计算中发挥重要作用.

设 $T \in E(\mathbb{F}_q)[n]$, $P \in \langle T \rangle$, n 为素数, $n|q-1$. 利用 Tate-Lichtenbaum 对可将 E 上的离散对数计算化为 $\mathbb{F}_q^*$ 上的离散对数计算. 计算 $\alpha = \Phi_n(T,T)$, $\beta = \Phi_n(T,p)$. 若 α 为 n 次本原单位根, 在 $\mathbb{F}_q^*$ 上计算离散对数 m, 使得 $\beta = \alpha^m$, 就可得到 $P = mT$. 由于 n 为素数, α 为 n 次本原单位根 (即 $\alpha \neq 1$) 的概率为 $1 - \frac{1}{n}$.

在利用 MOV 约化时, 首先要求找到 k, 使得 $E[n] \subset E(\mathbb{F}_{q^k})$, 然后将 E 上的离散对数的计算化为 $\mathbb{F}_{q^k}^*$ 上离散对数的计算. 在使用 FR 约化时, 仅要求 $n|q-1$, 并不要求 $E[n] \subset E(\mathbb{F}_q)$, 所以 FR 约化可以在 $E[n] \not\subset E(\mathbb{F}_q)$ 的情形下使用. 由于 $n|\#E(\mathbb{F}_q) = q + 1 - t$, 可知 $t \equiv 2 \pmod{n}$, t 为 $\mathbb{F}_q$ 上 q 阶 Frobenius 变换的迹.

当 n 为素数, $n \nmid q$, $n \nmid q-1$ 时, 条件 $E[n] \subset E(\mathbb{F}_{q^k})$ 等价于条件 $n|q^k - 1$(参见文献 [33]), 这时使用 MOV 约化和使用 FR 约化要求的条件是相同的.

§15.6　SSSA 约化

在 FR 约化和 MOV 约化中, 循环群 $\langle P \rangle$ 同构嵌入 $\mathbb{F}_q$(或其扩域 $\mathbb{F}_{q^k}$) 的乘法群中, 从而将 $\langle P \rangle$ 上离散对数的计算化为 $\mathbb{F}_q^*$(或 $\mathbb{F}_{q^k}^*$) 上离散对数的计算. 本节介绍

Smart-Semaev-Satoh-Araki [34~36] 提出的计算 ECDLP 的方法, 它将群 $\langle P\rangle$ 同构嵌入 $\mathbb{F}_q^+$ ($\mathbb{F}_q$ 的加法群), 从而将 $\langle P\rangle$ 上离散对数的计算化为 $\mathbb{F}_q^+$ 上离散对数的计算.

设 $q=p^m$, $p\neq 2,3$ 为素数, $E/\mathbb{F}_q$ 由方程 $y^2=x^3+ax+b$ 定义, $P\in E(\mathbb{F}_q)$ 的阶为 p. 这类曲线称为异常 (anomalous) 椭圆曲线, 当 $q=p$ 时, 异常曲线上的 p 阶 Frobenius 变换的迹 $t=1$.

任一点 $Q=(x_Q,y_Q)\in E(\mathbb{F}_q)$, 当 D 不是 2 阶点和无穷远点时, Q 的单值化子 $t_Q=x-x_Q$; 当 $Q=(x_Q,0)$ 为 2 阶点时, $t_Q=y$; 当 $Q=\mathcal{O}$ 时, $t_Q=x/y$.

引理 15.2 设 $f\in\overline{F}_q(E)$, $\mathrm{div}(f)=pD$, D 不是主除子. 令 $f'=df/dx$, 则 $\mathrm{div}(f')=\mathrm{div}(f)-\mathrm{div}(y)$.

证明 当 D 不是主除子时, f' 不恒为零. 设 $D=\sum n_Q(Q)$, 则 $f=t_Q^{pn_Q}f_1$, $\mathrm{ord}_Q(f_1)=0$. 当 Q 不是 2 阶点和无穷远点时, $df/dx=df/dt_Q=t_Q^{pn_Q}df_1/dt_Q$, 从而 $\mathrm{ord}_Q(f')=pn_Q+m_Q$, 其中 $m_Q=\mathrm{ord}_Q(df_1/dt_Q)\geqslant 0$. 当 Q 为 2 阶点时,

$$df/dx=df/dy\cdot dy/dx=y^{pn_Q}((3x^2+a)/2y)df_1/dy,$$

由于 $\mathrm{ord}_Q\big((3x^2+a)/2y\big)=-1$, 故 $\mathrm{ord}_Q(f')=pn_Q-1+m_Q$, 其中 $m_Q=\mathrm{ord}_Q(df_1/dy)\geqslant 0$; 当 $Q=\mathcal{O}$ 时,

$$df/dx=df/d(x/y)\cdot d(x/y)/dx=(x/y)^{pn_Q}\big((-x^3+ax+2b)/2y^3\big)\cdot df_1/d(x/y),$$

由于 $\mathrm{ord}\big((-x^3+ax+2b)/2y^3\big)=3$, 故 $\mathrm{ord}_Q(f')=pn_Q+3+m_Q$, 其中 $m_Q=\mathrm{ord}_Q(df_1/d(x/y))\geqslant 0$. 我们有

$$\mathrm{div}(y)=(S_1)+(S_2)+(S_3)-3(\mathcal{O}),$$

其中 S_1,S_2,S_3 为 E 上 3 个 2 阶点, 故 $\mathrm{div}(f')=\mathrm{div}(f)-\mathrm{div}(y)+D_1$, 其中 $D_1=\sum m_Q(Q)$, 可见 D_1 是主除子, 所有的 m_Q 均为零, 证毕.

取一固定点 $R\in\langle P\rangle$, $R\neq Q$. 对任一 $Q\in\langle P\rangle$, 存在函数 $f_Q\in\mathbb{F}_q(E)$, 使得 $\mathrm{div}(f_Q)=p(Q)-p(\mathcal{O})$. 定义映射

$$\begin{aligned}\Phi:\ \langle P\rangle &\longrightarrow \mathbb{F}_q^+,\\ Q &\longmapsto (f_Q'/f_Q)(R),\ (Q\neq\mathcal{O})\quad \mathcal{O}\longmapsto 0.\end{aligned}$$

定理 15.7 $\Phi(Q)$ 的定义是有意义的, Φ 是 $\langle P\rangle$ 到 $\mathbb{F}_Q^+$ 的同构嵌入.

证明 从引理 15.2 得到 $\mathrm{div}(f_Q'/f_Q)=-\mathrm{div}(y)$, R 不是 2 阶点和无穷远点, 所以 $\Phi(Q)$ 是 $\mathbb{F}_q^+$ 中的非零元, 仅需证 Φ 是同态映射.

设除子 D' 与 $D=(Q)-(\mathcal{O})$ 线性等价, 则存在函数 g, 使得 $\mathrm{div}(g)=D-D'$, 若 $\mathrm{div}(f)=pD'$, 易见 $f_Q=f\cdot g^p$, 这时 $f'/f=f_Q'/f_Q$. 在定义 $\Phi(Q)$ 时可以任取一个与

D 线性等价的除子代替 D. 设 $Q_i \in \langle P\rangle$, $D_i = (Q_i) - (\mathcal{O})$, $\mathrm{div}(f_{Q_i}) = pD_i$, $i = 1, 2$. 令 $D_{Q_1+Q_2} = D_1 + D_2 = (Q_1) + (Q_2) - 2(\mathcal{O}) \sim (Q_1 + Q_2) - (\mathcal{O})$, 取函数 $f_{Q_1+Q_2}$, 使得 $\mathrm{div}(f_{Q_1+Q_2}) = pD_{Q_1+Q_2} = \mathrm{div}(f_{Q_1} \cdot f_{Q_2})$, $f_{Q_1+Q_2}$ 与 $f_{Q_1} \cdot f_{Q_2}$ 仅差一个常数因子, 故

$$f'_{Q_1+Q_2}/f_{Q_1+Q_2} = f'_{Q_1}/f_{Q_1} + f'_{Q_2}/f_{Q_2}.$$

Φ 是同态映射, 证毕.

考虑如何计算 $\Phi(Q)$. 取 2 阶点 S, 存在函数 f_Q, 使得 $\mathrm{div}(f_Q) = p(Q+S) - p(S) \sim p(Q) - p(\mathcal{O})$. 由上述可知 $\Phi(Q) = (f'_Q/f_Q)(R)$. 在 $\langle P\rangle \times \mathbb{F}_q^+$ 上定义一个运算

$$(Q_1, a_1) \oplus (Q_2, a_2) = (Q_1 + Q_2, a_1 + a_2 + (h'/h)(R)),$$

其中函数 h 适合

$$\begin{aligned}\mathrm{div}(h) &= (Q_1 + S) + (Q_2 + S) - (Q_1 + Q_2 + S) - (S) \\ &= \{(Q_1 + S) + (Q_2 + S) + (-Q_1 - Q_2 + S) - 3(S)\} \\ &\quad - \{(Q_1 + Q_2 + S) + (-Q_1 - Q_2 + S) - 2(S)\} \\ &= \mathrm{div}(\lambda_{Q_1,Q_2}) - \mathrm{div}(\eta_{Q_1+Q_2}).\end{aligned}$$

函数 $\lambda_{Q_1,Q_2}(X+S)$ 和 $\eta_{Q_1+Q_2}(X+S)$ 都是 x 和 y 的线性函数, 前者是通过 $Q_1, Q_2, -(Q_1+Q_2)$ 的直线, 后者是通过 $Q_1+Q_2, -(Q_1+Q_2)$ 的直线. 我们有

$$h'/h = \lambda'_{Q_1,Q_2}/\lambda_{Q_1,Q_2} - \eta'_{Q_1+Q_2}/\eta_{Q_1+Q_2}.$$

等式右端的两项可用下述方法计算: 设 $\delta(X) = Ax + By + C$ $(A, B, C \in \mathbb{F}_q)$ 是上述提及的直线, 令 $\delta_1(X) = \delta(X - S)$, 我们欲计算 δ_1'/δ_1, 易见

$$\delta' = A + Bdy/dx = A + B(3x^2 + A)/2y$$

及 $d\delta = 2y\delta' dx/2y$, 通过直接计算可以发现 $dx/2y(X - S) = dx/2y$(事实上, $dx/2y$ 在任一平移变换下不变, 见文献 [12], 第三章命题 5.1), 所以

$$d\delta(X - S) = (2y\delta')(X - S)(dx/2y)(X - S) = (2y\delta')(X - S) \cdot dx/2y,$$

故

$$(\delta_1'/\delta_1)(X) = d\delta(X - S)/dx \cdot \delta(X - S)^{-1} = (2y\delta')(X - S)/2y\delta(X - S). \quad (15.3)$$

当以 $X = R$ 代入时, $R - S$ 不是 2 阶点和无穷远点, 上式右端为 $\mathbb{F}_q^+$ 中的非零元.

设 $p = \alpha_0 + 2\alpha_1 + \cdots + 2^t\alpha_t$ $(\alpha_i = 0, 1)$, 从 $(Q, 0)$ 出发, 依次计算 $(2Q, a_1), \cdots, (2^tQ, a_t)$, 然后计算 $\alpha_0(Q, 0) \oplus \alpha_1(2Q, a_1) \oplus \cdots \oplus \alpha_t(2^tQ, a_t) = (\mathcal{O}, (f'_Q/f_Q)(R))$. 可见 $\Phi(Q)$ 的计算量为 $O(\log p)$.

若 $Q \in \langle P \rangle$, $Q = lP$, 则由 $\Phi(Q) = l\Phi(P)$ 可得 $l = \Phi(Q) \cdot \Phi(P)^{-1}$.

事实上, 为了通过 (15.3) 式计算 $\Phi(Q)$, 可取 E 上任一不在 $\langle P \rangle$ 中的点代替 S. 但由于 2 阶点 $S = (\alpha, 0)$, α 适合方程 $x^3 + ax + b = 0$, 所以 $\mathbb{F}_q(\alpha)$ 最多为 $\mathbb{F}_q$ 的 3 次扩张, 选用 2 阶点时上述所有计算可以在 $\mathbb{F}_{q^3}$ 中完成.

文献 [37] 给出了异常曲线上 DLP 的另一种算法, 它可以保证所有的计算在 $\mathbb{F}_q$ 中完成. 取 $R = \mathcal{O}$, 对任一 $Q \in \langle P \rangle$; $Q \neq \mathcal{O}$, 取函数 $f_Q \in \mathbb{F}_q(E)$, 使得

$$\operatorname{div}(f_Q) = p(Q+P) - p(P). \tag{15.4}$$

定义映射

$$\begin{aligned} \Psi:\ \ \langle P \rangle &\longrightarrow \mathbb{F}_q^+, \\ Q &\longmapsto \Big(\frac{df_Q/dt}{f_Q}\Big)(\mathcal{O}),\ Q \neq \mathcal{O}, \\ \mathcal{O} &\longmapsto 0, \end{aligned}$$

其中 $t = x/y$ 为 $\mathcal{O}$ 的单值化子 (注意: 这里用 df_Q/dt 代替 df_Q/dx), f_Q 在 $\mathcal{O}$ 处有展开式

$$f_Q = \begin{cases} a_0 + a_1 t + O(t^2), & Q \neq -P, \\ t^p\big(b_0 + b_1 t + O(t^2)\big), & Q = -P. \end{cases}$$

由 (11.4) 式, 可知 $a_0 \neq 0$, $b_0 \neq 0$, 易见

$$\Psi(Q) = \begin{cases} a_1/a_0, & Q \neq -P, \\ b_1/b_0, & Q = -P. \end{cases}$$

类似于定理 15.7, 可以证明 Ψ 是 $\langle P \rangle$ 到 $\mathbb{F}_q^+$ 的同态, 由引理 15.2,

$$\begin{aligned} \operatorname{ord}_{\mathcal{O}}(df_P/dt) &= \operatorname{ord}_{\mathcal{O}}(df_P/dx) - \operatorname{ord}_{\mathcal{O}}(dt/dx) \\ &= \operatorname{ord}_{\mathcal{O}}(f_P) - \operatorname{ord}_{\mathcal{O}}(y) - \operatorname{ord}_{\mathcal{O}}(dt/dx) \\ &= \operatorname{ord}_{\mathcal{O}}(f_P) \neq 0 \end{aligned}$$

(这里利用了 $\operatorname{ord}_{\mathcal{O}}(y) = -\operatorname{ord}_{\mathcal{O}}(dt/dx) = 3$), 可见 $\Psi(P) \neq 0$, Ψ 是 $\langle P \rangle$ 到 $\mathbb{F}_q^+$ 的同构嵌入. 也可以得到与计算 $\Phi(Q)$ 类似的计算 $\Psi(Q)$ 的算法.

§15.7 有限域上离散对数的计算

MOV 约化和 FR 约化, 将计算 $\mathbb{F}_q$ 上的椭圆曲线离散对数化为计算有限域乘法群 $\mathbb{F}_{p^k}^*$ 上的离散对数, 这里约定 $p \neq 2, 3$ 为一个素数. 本节介绍计算 $\mathbb{F}_{p^k}^*$ 上的离散对数的指标计算法 (index calculus method), 并证明它是一个亚指数算法.

首先介绍一般的 n 阶循环群 G 上的指标计算法. 设 g 为 G 的生成元, $p_1, \cdots, p_m$ 为 G 中 m 个元素. 算法的第 1 步是设法找到足够多的关系式

$$\prod_{j=1}^{m} p_j^{a_{ij}} = g^{b_i}, \tag{15.5}$$

由此得到一组线性同余式

$$\sum_{j=1}^{m} a_{ij} \mathrm{ind}_g p_j = b_i \pmod n, \tag{15.6}$$

假定从这组同余式可以解得 $\mathrm{ind}_g p_j$ $(1 \leqslant j \leqslant m)$, 算法的第 2 步是解这组同余式. 设 a 为 G 中任一元素, 算法的第 3 步是计算 $\mathrm{ind}_g a$. 设法找到一个正整数 e, 使得

$$\prod_{j=1}^{m} p_j^{e_j} = ag^e,$$

由此可得到 $\mathrm{ind}_g a = \sum_{j=1}^{m} e_j \, \mathrm{ind}_g p_j - e$. 算法的前两步是预运算. 当要计算某一元素的离散对数时, 仅需要进行第 3 步. 第 3 步所需要的时间比前两步要少得多.

对于一般的群 G, 指标计算法并不一定是可行的, 因为并不一定能找到足够多的关系式 (15.5). 该方法在 $\mathbb{F}_{p^k}^*$ 上是可行的.

首先考虑 $k = 1$ 的情形, 即 $\mathbb{F}_p^*$ 上的指标算法. 设 $p_1, p_2, \cdots, p_m$ $(< p)$ 为最小的 m 个素数. 算法的第 1 步是寻找关系式 (15.5), 随机取整数 $b \in [1, p-1]$, 计算最小的正整数 r, 使得 $r \equiv g^b \pmod p$, 这里 g 是模 p 的原根. 用 $p_1, \cdots, p_m$ 依次试除 r, 如果 r 是这 m 个素数的乘积, 则找到一个我们所要的关系式, 这时称 r 是一个光滑数, 或称 r 是 ρ_m 光滑的. 找到一个光滑数就找到一个关系式 (15.5).

显然, m 越大, r 为光滑数的机会就越大, 在算法的第 1 步找出足够的光滑数所需的计算量就会减少. 但在算法的第 2 步, 求解关于 $\mathrm{ind}_g p_i$ 的线性方程组的计算量就会增加, 证明 r 是光滑数的计算量也会增加, 因此需要选取适当的 m, 优化所需的总的计算量.

设 x, y 为正整数, 令

$$\varphi(x, y) = \#\{a \in \mathbb{Z} | 1 \leqslant a \leqslant x, \ a\text{的所有素因子不超过}y\},$$

则随机取 b, 使得相应的 r 为光滑数的概率为 $\varphi(p, p_m)/p$. 由文献 [38] 的结果有

$$\varphi(x, y) = x \exp\left((-1 + o(1))\mu \log \mu\right),$$

其中 $\mu = \log x / \log y$, $\mu \to \infty$ 及 $y \geqslant \log^2 x$. 令

$$L(p) = \exp\left(\sqrt{\log p \log\log p}\right).$$

取 $p_m \approx L(p)^c$, 这里 c 为一常数, 由素数定理可见

$$m \approx p_m/\log p_m = L(p)^{c+o(1)}, \qquad \log p/\log p_m = c^{-1}\sqrt{\log p/\log\log p},$$

因而

$$\begin{aligned}\varphi(p,p_m)/p &= \exp\big((-1+o(1))\cdot c^{-1}\sqrt{\log p/\log\log p}(2^{-1}\log\log p \\ &\quad - 2^{-1}\log(\log\log p) - \log c)\big) \\ &= L(p)^{-1/2c+o(1)}.\end{aligned}$$

所以平均随机选取 $L(p)^{1/2c+o(1)}$ 个 b 后, 可以得到 (15.5) 式的一个关系式, 欲得 $2m$ 个关系式, 需选取

$$2mL(p)^{1/2c+o(1)} = L(p)^{c+1/2c+o(1)}$$

个 b 值. 当 b 值选定后, 最多做 $m+\log p$ 次试除, 可以确定相应的 r 是否是光滑数 (若 $r=\prod_{i=1}^m p_i^{a_i}$, 则 $\sum_{i=1}^m a_i \leqslant \log r < \log p$). 所以指标计算法第 1 步的计算量为 $L(p)^{2c+1/2c+o(1)}$ 次 $\mathbb{F}_p$ 中的运算.

我们假定得到 $2m$ 个 (15.5) 式中的关系式后, 通过求解线性同余方程组 (15.6), 可以得到 $\mathrm{ind}_g p_i$ $(1 \leqslant i \leqslant m)$, 这假定看来是合理的, 但不可能严格证明. 在求解线性同余方程组时, 需要利用中国剩余定理将模 $p-1$ 的方程组化为模 $p-1$ 素因子 q 的方程组. 利用高斯消去法求解素域 $\mathbb{F}_q$ 上 m 阶线性方程组的计算量为 $O(m^3)$. 在得到 $\mathbb{F}_q$ 上的解后, 可以进一步得到模素数幂 q^l(这里 $q^l \| p-1$) 的解. 所以指标计算法的第 2 步所需计算量为 $O\big(L(p)^{3c+o(1)}\big)$.

设 $a \in \mathbb{F}_p^*$, 在算法的第 3 步计算 $\mathrm{ind}_g a$, 任取整数 e, 使得 $r \equiv ag^e \pmod p$ 为光滑数. 利用上述第 1 步中所做的分析, 可知第 3 步的计算量为 $O\big(L(p)^{c+1/2c+o(1)}\big)$.

若取 $c=1/2$, 由上述分析, 可见 $\mathbb{F}_p^*$ 上指标计算法的计算量为 $O\big(L(p)^{2+o(1)}\big)$, 当 $p\to\infty$ 时, 它是一个亚指数算法.

现在考虑 $\mathbb{F}_{p^k}^*$ 上的指标计算法. 我们将证明当 p 固定, $k\to\infty$ 时该算法是一个亚指数算法 (参阅文献 [39]).

设 g 为 $\mathbb{F}_{p^k}^*$ 的生成元, 则 $g' = g^{(p^k-1)/p-1}$ 是 $\mathbb{F}_p^*$ 的生成元. 假定已知 $\mathbb{F}_p^*$ 中任一元素是以 g' 为基的对数, 例如, 这可由上述 $\mathbb{F}_p^*$ 上的指标计算法得到. 我们把 $\mathbb{F}_p$ 中的元素称为纯量元. $\mathbb{F}_{p^k}^*$ 中任一元素都可惟一地用 $\mathbb{F}_p$ 上的一个次数小于 k 的多项式表示, 设 $m<k$ 为正整数 (其数值将在下面确定), 以 S_m 表示 $\mathbb{F}_p$ 上的所有次数大于零且不超过 m 的首 1 不可约多项式的集合, $P(m)$ 表示 S_m 中多项式的个数. 在指标计算法中, 这组多项式将具有在上述 $\mathbb{F}_p$ 的情形下, 最初的 m 个素数 $p_1,\cdots,p_m$ 同样的作用.

定义 15.3 $\mathbb{F}_p$ 上的一个多项式若能分解为一个纯量元和若干个次数不超过 m 的首 1 不可约多项式之乘积, 则称该多项式 (相对 m) 是光滑的. $\mathbb{F}_{p^k}^*$ 中的一个元素若可用光滑多项式表示, 则称该元素是光滑的.

$\mathbb{F}_{p^k}^*$ 上指标计算法的第 1 步是要找到 $\mathbb{F}_{p^k}^*$ 中足够多的光滑元. 设

$$\alpha = g^b = cR$$

是一个光滑元, R 是 $\mathbb{F}_p$ 上的一个首 1 多项式, 我们把 R 也理解为一个 $P(m)$ 维向量, 其分量为 R 的因子分解式中对应 S_m 中每个不可约因子的指数, 纯量 c 的对数, 当 p 较小时, 可用列表法给出, 当 p 很大时, 如上所述, 可用 $\mathbb{F}_p^*$ 上的指标计算法得到.

引理 15.3 $\mathbb{F}_{p^k}$ 中相对 m 的光滑元至少有 $\binom{P(m)+u}{u}$ 个, 其中 $u = \lfloor \frac{k-1}{m} \rfloor$.

证明 在 S_m 中任取 u 个或少于 u 个不可约多项式, 它们的乘积的次数不超过 $u \cdot m \leqslant k-1$, 因而对应 $\mathbb{F}_{p^k}$ 中的一个光滑元. 如果在集合 S_m 中添加一个元素 "1", 则我们在 $S_m \cup \{1\}$ 中任取 u 个元素 (可以重复取同一元素), 每次都得到一个不同的光滑元, 如此取法的个数为函数

$$f(x) = (1-x)^{-(P(m)+1)}$$

关于 x 的展开式中 x^u 项的系数, 即为

$$\frac{1}{u!} \cdot \frac{d^u}{dx^u} f(x)\Big|_{x=0} = \frac{(P(m)+1)(P(m)+2)\cdots(P(m)+u)}{u!} = \binom{P(m)+u}{u}.$$

证毕.

引理 15.4 当 $m \geqslant 1$ 时, $\frac{p^m}{2m} \leqslant P(m) \leqslant p^{m+1}$.

证明 后一不等式是显然的, 因为 m 次多项式共有 p^{m+1} 个. 以 $I(i)$ 表示 i 次首 1 不可约多项式的个数, 则

$$P(m) = \sum_{i=1}^{m} I(i) \geqslant I(m).$$

Berlekamp 在文献 [40] 中证明了

$$I(m) \geqslant \frac{p^m}{m}(1 - p^{1-m/2}),$$

所以当 $m \geqslant 4$ 时, 有

$$I(m) \geqslant \frac{p^m}{m}\left(\frac{1}{2}\right),$$

即证明了引理中的前一个不等式. 还需考虑 $m=1,2,3$ 的情形, 利用公式

$$I(m)=\frac{1}{m}\sum_{d|m}\mu(d)p^{m/d}$$

(见文献 [41] 定理 3.25) 得

$$I(1)=p,\qquad I(2)=\frac{1}{2}(p^2-p)\geqslant\frac{p^2}{4},\qquad I(3)=\frac{1}{3}(p^3-p)\geqslant\frac{p^3}{6}.$$

引理证毕.

从算法第 1 步得到一组光滑元 R_i $(1\leqslant i\leqslant I)$, 如何保证能在第 2 步从线性同余方程组 (15.6) 解出 $\mathrm{ind}_g f$ $(f\in S_m)$, 这是一个较困难的问题, 为此我们引入下述定义, 将有助于达到上述目的:

定义 15.4 随机生成的矢量组 $\{R_i\}(1\leqslant i\leqslant I)$ 称为事实上的支架集合, 如果再按同样的随机方式生成任一矢量 R, R 可表为 $\{R_i\}$ 的 (整系数) 组合的概率大于 1/2.

令 $l=k\cdot\ln p$, 这里 $\ln p$ 是以 2 为底的对数, l 是表示 $\mathbb{F}_{p^k}$ 中每一元素所需的比特长度. 令

$$m=\left\lfloor\frac{1}{\ln p}\sqrt{\frac{1}{3}l\cdot\ln(2k)}\right\rfloor,\tag{15.7}$$

在以下定理 15.9 的证明中, 将说明这样的 m, 可以在估计计算量时得到最优的上界.

令 $r_1=4P(m), r_2=2r_1/\varepsilon$, 其中 $\varepsilon=\binom{P(m)+u}{u}/p^m$, ε 是任取整数 b 使 g^b 为光滑元的概率的下界. 随机选取最多 r_2 个 b, 要求从诸 g^b 中找出 r_1 个光滑元, 设置 I 的初始值为零, 假设已经找到了光滑元 $\{R_i\}$ $(1\leqslant i\leqslant I)$, 这时再任取 b, 计算 $g^b=cR$, 若 R 是光滑元, 但不能表为 $\{R_i\}$ $(1\leqslant i\leqslant I)$ 的组合 (理解为向量), 则将 R 添加进 $\{R_i\}$, 并将 I 增加 1. 要求在选取 r_2 个 b 后, 能得到一个事实上的支架集, 将计算结果结束时的 I 记为 $I_{\max}$.

定理 15.8 当 $l\to\infty$ 时, 集合 $\{R_i\}(1\leqslant i\leqslant I_{\max})$ 不是事实上的支架集的概率趋于零.

证明 我们的算法失败, 可能有两种情形:

(1) 在 r_2 次尝试中没有可能找到 r_1 个光滑元.

(2) 从 r_1 个光滑元中产生的 $\{R_i\}(1\leqslant i\leqslant I_{\max})$ 不是事实上的支架集合.

现在分别估计这两个事件出现的概率的上界 P_1 和 P_2.

假定每次试验的成功概率为 δ, 在 N_2 次独立试验中, 成功的次数少于 N_1 的概率 P 适合

$$P\leqslant\frac{\delta(1-\delta)}{N_2(N_1/N_2)^2}\tag{15.8}$$

(这称为切比雪夫不等式).

考虑 P_1 的上界, 任取 b, 使得 g^b 为光滑元的概率至少为 ε. 利用 (15.8) 式取 $\delta=\varepsilon$, $N_1=r_1$, $N_2=r_2$ 得到

$$P_1 \leqslant \frac{\varepsilon(1-\varepsilon)}{b_2(b_1/b_2)^2} < \frac{b_2\varepsilon}{b_1^2} = \frac{1}{2P(m)}.$$

考虑 P_2 的上界, 我们把一个新向量添加进原有的 $\{R_i\}$ 理解为一次成功的试验, 所以每次试验成功概率是不同的, 它依赖于原有的 $\{R_i\}$, 但当 $\{R_i\}(1\leqslant i\leqslant I_{\max})$ 不是事实上的支架集时, 每次试验的成功概率至少为 $1/2$. 每个 R_i 是 $P(m)$ 维向量, 所以成功试验的次数一定少于 $P(m)$, 取 $\delta=1/2, N_1=P(m), N_2=r_1$, 由 (15.8) 式得

$$P_2 \leqslant \frac{1}{P(m)}.$$

由 (15.7) 式及引理 15.4, 当 $l\to\infty$ 时, 可知 $P_1+P_2\to 0$, 证毕.

定理 15.9 设 m 由(15.7)式给定, σ 为任一正数, 构造 $\{R_i\}(1\leqslant i\leqslant I_{\max})$ 需要

$$O\big(\exp\{(1+\sigma)\sqrt{12l\cdot\ln(2k)}\}\big)$$

次 $\mathbb{F}_{p^k}$ 中的运算, 其中 $l=k\cdot\ln p$.

证明 算法的第 1 步, 任取 r_2 个 b_i, 然后判断它是否是光滑元. 计算 g^{b_i} 的计算量为 $\ln b_i$ 阶, 这部分计算量可以忽略不记. 判断 g^{b_i} 是否是光滑元, 需用 S_m 中多项式逐个试除, 而由于 g^{b_i} 有重复因子, 增加的试除次数不超过 k, 所以总的试除次数不超过 $P(m)+k$, 算法第 1 步的计算量为 $O\big(r_2[P(m)+k]\big)$.

在算法的第 2 步, 每得到一个新的光滑元 $g^{b_i}=cR$, 都要用高斯法检查 R 是否可以是已有 $\{R_i\}$ 的线性组合, R_i 的维数为 $P(m)$, 所以第 2 步的计算量为 $O\big(r_1[P(m)]^3\big)$, 因此构造 $\{R_i\}(1\leqslant i\leqslant I_{\max})$ 的预运算总的计算量为

$$O\big(r_2[P(m)+k]\big)+O\big(r_1[P(m)]^3\big). \tag{15.9}$$

估计上式中两个量的上界, 由引理 15.4 及 (15.7) 式中 m 的选取, 可知 $P(m)\geqslant k$, 所以

$$O\big(r_2[P(m)+k]\big)=O\left(P(m)^2p^k\frac{u!P(m)!}{(P(m)+u)!}\right),$$

利用 Stirling 公式, $n!\sim\sqrt{2n\pi}\left(\frac{n}{e}\right)^n$ $(n\to\infty)$, 上式右端可化为

$$O\left(P(m)^2p^k\cdot\frac{u^uP(m)^{P(m)}}{(P(m)+u)^{P(m)+u}}\right)=O\left(P(m)^2p^k\cdot\frac{u^u}{P(m)^u}\right).$$

再利用引理 15.4 及 $(k/m)-1 \leqslant u < k/m$, 上式右端化为

$$O\Big(\frac{p^{2m+k}(k/m)^{k/m}}{(p^m/2m)^{(k/m)-1}}\Big) = O\big(p^{3m}(2k)^{k/m}\big) = O\Big(\exp\Big\{3m\ln p + \frac{k}{m}\ln(2k)\Big\}\Big). \quad (15.10)$$

当 $m = \frac{1}{\ln p}\sqrt{(1/3)l\cdot\ln(2k)}$ 时, 上式达到最小值, 由于 m 为整数, 故取 m 为 (15.7) 式右端给定的值.

对任一 $\delta > 0$, 当 m 足够大时有

$$\frac{1}{(1+\delta)\ln p}\sqrt{(1/3)l\cdot\ln(2k)} \leqslant m \leqslant \frac{1}{\ln p}\sqrt{(1/3)l\cdot\ln(2k)},$$

将上式代入 (15.10) 式, 得到 (15.9) 式中第 1 项的上界

$$O\Big(\exp\Big\{\sqrt{3l\cdot\ln(2k)} + \frac{(1+\delta)k\ln p\ln(2k)}{\sqrt{(1/3)l\cdot\ln(2k)}}\Big\}\Big) = O\Big(\exp\big\{(1+\delta)\sqrt{12l\cdot\ln(2k)}\big\}\Big).$$

(15.9) 式中第 2 项的上界可以类似地得到:

$$O\big(b_1P(m)^3\big) = O\big(P(m)^4\big) = O\big(p^{4m}\big) = O\big(\exp\{4\sqrt{(1/3)l\cdot\ln(2k)}\}\big).$$

定理证毕.

由定理 15.9 可见, 当 p 固定, $k \to \infty$ 时, $\mathbb{F}_{p^k}$ 上的指标计算法是一个亚指数算法, 从定理 15.9 的证明也可知道, 寻找光滑元的计算量大于求解线性方程组的计算量.

在基于离散对数的公钥密码方案的设计中, 最常用的基群是 $\mathbb{Z}_p^*$. 以上已经介绍了 $\mathbb{Z}_p^*$ 的指标计算法, 然而数域筛法是目前求 $\mathbb{Z}_p^*$ 上离散对数的最快算法. 在用数域筛法分解大数的思想启发下, 1992 年, Gordon[42] 首先设计了求 $\mathbb{Z}_p^*$ 上离散对数的数域筛法, 且估计算法的时间复杂度为 $L_p[1/3, 3^{1/2}]$; 1993 年 Schirokauer[43] 改进了 Gordon 的方法, 使期望时间复杂度达到 $L_p[1/3, (64/9)^{1/3}]$.

我们已经知道, 利用 §15.2 和 §15.3 的方法计算 $\mathbb{Z}_p^*$ 上离散对数的时间复杂度为 $O(\sqrt{q})$, 其中 q 是 $p-1$ 中的最大素因子. 为保障最大的安全强度, 实际应用中 q 一般取和 p 相当的素数, 即 $p-1 = rq$, r 是一个很小的数. 此时求 $\mathbb{Z}_p^*$ 上离散对数 $x = \log_u v$, 只需求 $x_1 \equiv x \pmod r$ 和 $x_2 \equiv x \pmod q$, 然后用中国剩余定理求得 $x = \log_u v$. 下面介绍用数域筛法求

$$x = \log_u v \pmod q.$$

数域筛法的目的是求得整数 s 和 t, 且 $\gcd(t,q) = 1$, 使得 $u^s v^t$ 为 $\mathbb{Z}_p^*$ 中的 q 次幂, 即

$$u^s v^t = w^q,$$

则

$$x \equiv -st^{-1} \pmod q.$$

因此, 我们的思路是构造 $\mathbb{Z}_p^*$ 中的一个 q 次方幂, 使其能够写成 u 和 v 的次幂之乘积. 和大数分解的数域筛法一样, 首先构造一个环 $\mathbb{Z}[\alpha]$ 中的 q 次幂, 然后通过某个到 $\mathbb{Z}_p$ 的环同态, 得到 $\mathbb{Z}_p$ 中的一个 q 次幂. 具体地, 选择一个首一的整系数不可约多项式 $f(x)$, 和一个自然数 $m = 2^h v$, 使得 $f(m) \equiv 0 \pmod p$, 且 q 不整除 $d(f)$. 令 α 是 $f(x)$ 的一个根, 数域 $K = \mathbb{Q}(\alpha)$, 因为 q 在 K 不分歧, 故

$$qO_K = \wp_1 \cdots \wp_g,$$

令 $\varepsilon_i = N(\wp_i) - 1$, $\varepsilon = \mathrm{lcm}\{\varepsilon_i | i = 1, \cdots, g\}$, 则对任意 $\omega \in O_K$, 有

$$\omega^\varepsilon \equiv 1 \pmod q,$$

这样可定义映射

$$\begin{aligned} \lambda: \quad \Gamma = \{\omega \in O_K | q \nmid N(\omega)\} &\longrightarrow \frac{qO_K}{q^2O_K} \\ \omega &\longmapsto \omega^\varepsilon - 1 \pmod{q^2O_K}, \end{aligned}$$

可验证 λ 是乘法半群 Γ 到加法群 $\frac{qO_K}{q^2O_K}$ 的同态.

引理 15.5 *令 U 是 O_K 的单位群, $U' = \{\eta \in U | \eta \equiv 1 \pmod{q^2O_K}\}$, 假设 $U' \subseteq U^q$, 且 K 的类数 h_K 不被 q 整除. 若 $\omega \in \Gamma$ 满足*

(1) $\mathrm{ord}_\wp(\omega) \equiv 0 \pmod q$, 对 O_K 中所有的素理想 $\wp$;

(2) $\lambda(\omega) = 0$;

则 ω 是 O_K 中 q 次方幂.

证明 由条件 (1) 可知, 存在理想 I, 使得 $(\omega) = I^q$, 又由于 q 不整除 h_K, 故 I 也是主理想, 设为 (δ), 则存在 $u \in U$, 使得 $\omega = \delta^q u$. 而 $\lambda(\omega) = 0$ 意味着 $\omega^\varepsilon \equiv 0 \pmod{q^2}$, 故 $1 \equiv \omega^\varepsilon = (\delta^\varepsilon)^q u^\varepsilon \equiv u^\varepsilon \pmod{q^2}$, 所以 $u \in U' \subseteq U^q$, 即 u 是一个 q 次方幂, ω 也是 O_K 中 q 次方幂, 证毕.

注意：假设 K 是随机选取的一个代数数域, 则 K 满足引理 15.5 的条件的概率是很大的, 详情可见文献 [43]. 在以下讨论中, 不妨设 K 满足引理 15.5 的条件.

取 O_K 的一组整基 $\{\alpha_1, \cdots, \alpha_n\}$, $\omega^\varepsilon - 1$ 能够写成 $q(a_1\alpha_1 + \cdots + a_n\alpha_n)$, $a_i \in \mathbb{Z}$, 定义同态映射

$$\begin{aligned} \lambda_i: \quad \Gamma &\longrightarrow \mathbb{Z}_q, \\ \omega &\longmapsto a_i \pmod q, \end{aligned}$$

故 $\lambda(\omega) = 0$ 当且仅当 $\lambda_i(\omega) = 0$, $i = 1, \cdots, n$.

筛法是构造集合 $S=\{(a,b)\,\big|\,|a|\leqslant s,\ 1\leqslant b\leqslant t,\ \gcd(a,b)=1,\ (a+bm)N(a+b\alpha)\ B-\text{光滑}\}$, 使得 $|S|\geqslant S_Q|+|S_K|+n-1$, 同大数分解数域筛法一样, 令 $g(x,y)=x+my$, $\overline{f}=y''f(-\frac{x}{y})$, 用筛法能寻找满足这两个齐次多项式的光滑值.

下面我们描述数域筛法的大致步骤:

(1) 选取 m, $f(x)$ 同上, 定义环同态

$$\begin{aligned}\phi:\ \ \mathbb{Z}[\alpha]\ &\longrightarrow\ \mathbb{Z}_p,\\ g(\alpha)\ &\longmapsto\ g(m),\end{aligned}$$

然后选择合适的一个界 B, 构造有理因子基 $FQ=\{p\text{素数}\,|\,p\leqslant B\}$, 代数因子基 $FK=\{\wp\subseteq\mathbb{Z}[\alpha]|\wp\text{是一次素理想},\ N(\wp)\leqslant B\}$.

(2) 筛法是构造集合 $S=\{(a,b)\,\big|\,|a|\leqslant s,\ 1\leqslant b\leqslant t,\ \gcd(a,b)=1,\ (a+bm)N(a+b\alpha)\ B-\text{光滑}\}$, 使得 $|S|\geqslant S_Q|+|S_K|+n-1$, 同大数分解数域筛法一样, 令 $g(x,y)=x+my$, $\overline{f}=y''f(-\frac{x}{y})$, 用筛法能寻找满足这两个齐次多项式的光滑值.

对每个 $(a,b)\in S$,

$$\Big|a+bm\Big|=\prod_{p\in S_Q}p^{e_p(a,b)},\qquad \Big|a+b\alpha\Big|=\prod_{\wp\in S_K}\wp^{e_\wp(a,b)}.$$

(3) 构造 $d=|S_Q|+|S_K|+n-1$ 维 $\mathbb{Z}_q$ 上的向量

$$\begin{aligned}\nu(a,b)&=\big(e_p(a,b)\bmod q, e_\wp(a,b)\bmod q, \lambda_j(a+b\alpha)\bmod q\big)_{p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n},\\ \nu(u)&=\big(e_p(u)\bmod q, e_\wp=0, \lambda_j=0\big)_{p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n},\\ \nu(v)&=\big(e_2=h,\ e_p=0,\ e_\wp(\alpha)=0,\ \bmod q,\ \lambda_j(a)\bmod q\big)_{2\neq p\in S_Q,\,\wp\in S_K,\,1\leqslant j\leqslant n}.\end{aligned}$$

从集合 $\{x(a,b)\,|\,(a,b)\in S\}$ 中选取 $(d-1)$ 个元素, 使其和 $\nu(u)$ 构成一组基

$$\Big\{\nu(a,b)\,\Big|\,(a,b)\in S'\subseteq S\Big\}\cup\big\{\nu(u)\big\},$$

然后将这 d 个向量作为列向量构成可逆矩阵 A, 解 $\mathbb{Z}_q$ 上的线性方程组

$$AX=-\nu(v)',$$

求得解 $\big(x(a,b),x(u)\big)_{(a,b)\in S'}$, 则由引理 15.5 可知 $\alpha\prod_{(a,b)\in S'}(a+b\alpha)^{x(a,b)}$ 是 $\mathbb{Z}[\alpha]$ 中的 q 次方幂, $u^{x(u)}2^h\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\pmod p$ 是 $\mathbb{Z}_p$ 中的 q 次幂. 而

$$u^{x(u)}2^h\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\equiv u^{x(u)}v^{-1}m\prod_{(a,b)\in S'}(a+bm)^{x(a,b)}\pmod p,$$

故

$$\log_u(v) \equiv x(u) \pmod{q}.$$

Adelman[44] 将数域筛法类比到函数域中, 提出函数域筛法来求 $\mathbb{F}_{p^m}^*$ 上的离散对数, 只要 p 不是很大, 函数域筛法的期望时间复杂度为 $L_{p^m}[1/3, c]$, $c > 0$ 是一个常数, 且当 p 取 2 时, 该算法恰是 Coppersith 算法[45].

第十六章　超椭圆曲线离散对数的指标计算法

§16.1　超椭圆曲线的 Jacobian

为了简化, 假设域 F 的特征不等于 2(特征为 2 的情形见文献 [46]). 假设定义在 F 上的多项式

$$f(x) = x^{2g+1} + a_1 x^{2g} + \cdots + a_{2g+1}$$

没有重根. 方程

$$y^2 = f(x) \tag{16.1}$$

在仿射平面上定义一条曲线, 该曲线上各点都是非奇异的. 将方程 (16.1) 化为齐次方程

$$Y^2 Z^{2g-1} = X^{2g+1} + a_1 X^{2g} Z + \cdots + a_{2g+1} Z^{2g+1},$$

可见上述曲线在射影平面上完备化后, 增加惟一的点 $\mathcal{O} = (0,1,0)$, 称为无穷远点, 当 $g > 1$ 时, 它是一个奇异点. 称射影曲线

$$\mathcal{C} = \{(\alpha, \beta) \mid \alpha, \beta \in \overline{F},\ \beta^2 = f(\alpha)\} \cup \{(0,1,0)\}$$

为亏格 g 的超椭圆曲线, 当 $g = 1$ 时, 它就是椭圆曲线. $\mathcal{C}$ 上除 $\mathcal{O}$ 之外的点都称为有限点.

设点 $Q = (\alpha, \beta) \in \mathcal{C}$, 则 $\overline{Q} = (\alpha, -\beta) \in \mathcal{C}$ 称为 Q 的反点. 当 $\beta \neq 0$ 时, $Q \neq \overline{Q}$, 这时 $f(\alpha) \neq 0$, 取 $x - \alpha$ 为 Q 点的单值化子 ($x - \alpha$ 在 Q 点有 1 阶零点). 当 $\beta = 0$ 时, $Q = \overline{Q}$, 这时 $f(\alpha) = 0$, 取 y 为 Q 的单值化子, 易见 $\mathrm{ord}_Q(x - \alpha) = 2$.

设 $p(x,y) \in \overline{F}[x,y]$, 由于 $y^2 = f(x)$, 作为 $\mathcal{C}$ 上的函数 $p(x,y)$ 可表为 $\overline{p}(x,y) = a(x) - b(x)y$, 其中 $a(x), b(x) \in \overline{F}[x]$. 考虑 $p(x,y)$ 在 $\mathcal{C}$ 的点 Q 的阶.

(i) 若 $Q = (\alpha, \beta)$ 为有限点. 设 $\overline{p} = (x-\alpha)^{r_0}(a_0(x) - b_0(x)y)$, $(x - \alpha)$ 不能同时整除 $a_0(x)$ 和 $b_0(x)$. 若 $a_0(\alpha) - b_0(\alpha)\beta \neq 0$, 则

$$\mathrm{ord}_Q P = \begin{cases} r_0, & Q \neq \overline{Q}, \\ 2r_0, & Q = \overline{Q}. \end{cases}$$

若 $a_0(\alpha) - b_0(\alpha)\beta = 0$, 则

$$\mathrm{ord}_Q P = \begin{cases} r_0 + r, & Q \neq \overline{Q}, \\ 2r_0 + 1, & Q = \overline{Q}, \end{cases}$$

其中 $r > 0$ 适合

$$a_0(x) - b_0(x)y = \sum_{i=r}^{\infty} d_i(x-\alpha)^i.$$

r 可利用

$$(x-\alpha)^r \parallel a_0(x)^2 - b_0(x)^2 f(x) \tag{16.2}$$

决定. 由于 $b_0(\alpha) \neq 0$(若 $b_0(\alpha) = 0$, 则 $a_0(\alpha) = 0$, 不可能), 故 $b_0(x) \neq 0$, 有

$$\left(\frac{a_0(x)}{b_0(x)} - \frac{1}{b_0(x)} \sum_{i=r}^{\infty} d_i(x-\alpha)^i\right)^2 - f(x) = 0,$$

因而

$$a_0(x)^2 - b_0(x)^2 f(x) = 2a_0(x) \sum_{i=r}^{\infty} d_i(x-\alpha)^i - \left(\sum_{i=r}^{\infty} d_i(x-\alpha)^i\right)^2,$$

若 $(x-\alpha) \nmid a_0(x)$, 可见 (16.2) 式成立; 若 $(x-\alpha) \mid a_0(x)$, 由于 $(x-\alpha) \nmid b_0(x)$, 可见 $(x-\alpha)^2 \mid f(x)$, 但 $f(x)$ 没有重根, 这不可能.

当 $Q = \overline{Q}$ 时, $\beta = 0$, 这时 $a_0(\alpha) = 0$, $b_0(\alpha) \neq 0$. 因 y 是 Q 的单值化子, 可见 $\mathrm{ord}_Q(a_0(x) - b_0(x)y) = 1$, 且 $x - \alpha \parallel a_0(x)^2 - b_0(x)^2 f(x)$(注意 $x - \alpha \parallel f(x)$).

(ii) 若 $Q = \mathcal{O}$. 由于 $y^2 = x^{2g+1} + x$的低次项, 可取 $\mathrm{ord}_{\mathcal{O}}(x) = -2$, $\mathrm{ord}_{\mathcal{O}}(y) = -2g-1$, 所以

$$\mathrm{ord}_{\mathcal{O}} p = -\max(2\deg a(x), 2g+1+2\deg b(x)).$$

由 $\mathcal{C}$ 上的点 Q_i 组成的有限形式和 $D = \sum m_i Q_i \ (m_i \in \mathbb{Z})$ 称为 $\mathcal{C}$ 的一个除子, 所有除子组成加法群 $\mathcal{D}$. 除子 D 的次数 $\deg D = \sum m_i$, 所有次数为零的除子组成 $\mathcal{D}$ 的一个子群 $\mathcal{D}^\circ$. 当 $p(x,y)$ 在 $\mathcal{C}$ 上不恒为零时, 定义函数 $p(x,y) \in \overline{F}[x,y]$ 对应的除子 $\mathrm{div}\ (p) = \sum_Q \mathrm{ord}_Q(p)$, 由代数曲线的一般理论, 可知 $\mathrm{div}\ (p) \in \mathcal{D}^\circ$. 设 $p(x,y)/q(x,y)$ 为 $\mathcal{C}$ 上的有理函数, 当 p 和 q 不在 $\mathcal{C}$ 上恒为零时, 令 $\mathrm{div}\ (p/q) = \mathrm{div}\ (p) - \mathrm{div}\ (q)$. $\mathcal{C}$ 上任一有理函数对应的除子称为主除子, 由主除子生成 $\mathcal{D}^\circ$ 的子群记为 $\mathfrak{B}$. 商群 $\mathcal{D}^\circ/\mathfrak{P}$ 称为超椭圆曲线 $\mathcal{C}$ 上的 Jacobian. 除子 $D_1, D_2 \in \mathcal{D}^\circ$, 当 $D_1 - D_2 \in \mathfrak{P}$ 时, 记 $D_1 \sim D_2$, 称 D_1 与 D_2 线性等价.

设 $Q = (\alpha, \beta) \in \mathcal{C}$, 当 $\beta \neq 0$ 时, 有 $\mathrm{div}\ (x-\alpha) = Q + \overline{Q} - 2\mathcal{O}$, 所以 $-Q \sim \overline{Q} - 2\mathcal{O}$, 当 $\beta = 0$ 时, 有 $\mathrm{div}\ (x-\alpha) = 2Q - 2\mathcal{O}$, 所以 $2Q \sim 2\mathcal{O}$. 设 $D = \sum m_i Q_i$ 为 $\mathcal{D}^\circ$ 中任一除子, 利用上述性质, 可知 D 一定与一个形如 $\sum m_i Q_i - (\sum m_i)\mathcal{O}$ 的除子线性等价, 它具有下述性质: 每个系数 $m_i > 0$, 当 Q_i 在和式中出现时, $\overline{Q}_i (\neq Q)$ 一定不在和式中出现, 当 $Q_i = \overline{Q}_i$ 时, Q_i 的系数为 1. 具有这种性质的除子称为半既约的. 在一个半既约的除子中, 若 $\sum m_i \leqslant g$, 则称它为既约除子. 利用 Riemann-Roch 定理, 一定存在一个函数 f, 使 $D + (f) \geqslant -g\mathcal{O}$(因 $l(D + g\mathcal{O}) \geqslant g - g + 1 = 1$), 所以 $\mathcal{D}^\circ$ 中

任一除子一定与一个既约除子线性等价, 也可以证明这样的既约除子是惟一的 (见文献 [11]).

超椭圆曲线的 Jacobian 是一个加法群. 我们给 Jacobian 中每个元素一个恰当的表达式, 并找出它的加法的运算法则.

设 $D=\sum m_iQ_i-(\sum m_i)\mathcal{O}$ 是 $\mathcal{D}^\circ$ 中一个半既约除子, $Q_i=(\alpha_i,\beta_i)$. 令 $a(x)=\prod(x-\alpha_i)^{m_i}$, $b(x)\in\overline{F}[x]$ 适合下述条件: $b(\alpha_i)=\beta_i\quad(\forall i)$, $a(x)\parallel b(x)^2-f(x)$ ((16.2) 式), $\deg b(x)<\deg a(x)$, 这样的 $b(x)$ 是惟一确定的. 易见除子 D 线性等价于 $\gcd(\mathrm{div}(a(x)),\mathrm{div}(b(x)-y))$(不考虑 $\mathcal{O}$ 的部分). 为了简单起见, 今后我们表 $D=\mathrm{div}\ (a,b)$. 例如若 $Q=(\alpha,\beta)$, 则 $Q-\mathcal{O}=\mathrm{div}\ (x-\alpha,\beta)$, $2Q-2\mathcal{O}=\mathrm{div}\ \big((x-\alpha)^2,(f'(\alpha)(x-\alpha)+2\beta^2)/2\beta\big)$. 当且仅当 $\deg a(x)\leqslant g$ 时, $\mathrm{div}\ (a,b)$ 为既约除子.

设 $\mathrm{div}\ (a,b)=\mathrm{div}\ (a_1,b_1)+\mathrm{div}\ (a_2,b_2)$, 如何计算 a,b? 设 $d=\gcd(a_1,a_2,b_1+b_2)$(多项式的最大公因子), 存在 $s_1(x),s_2(x),s_3(x)\in\overline{F}[x]$, 使得

$$s_1a_1+s_2a_2+s_3(b_1+b_2)=d,$$

则

$$\begin{aligned}a&=a_1a_2/d^2,\\ b&=(s_1a_1b_2+s_2a_2b_1+s_3(b_1b_2+f))/d\mod a,\end{aligned}\tag{16.3}$$

可以直接验证上述计算公式是正确的[47], 该计算方法实际上是通过 (虚)2 次代数函数域 $\overline{F}(x,y)$ 中类群的加法得来的, 为了更好的理解这个算法, 我们将在下节讨论 $\overline{F}(x,y)$ 的类群的加法.

考虑两个特殊的情形:

(i) 当 a_1 与 a_2 互素时, $d=1$, 可取 $s_3=0$, 这时 $a=a_1a_2$, $b=s_1a_1b_2+s_2a_2b_1\mod a$.

(ii) 当 $a_1=a_2$, $b_1=b_2$(即计算一个除子的 2 倍) 时, 可取 $s_2=0$.

上述计算得到的 $\mathrm{div}\ (a,b)$ 不一定是既约的, 一般, 任一半既约的除子表达式可利用下述方法化为既约的表达式. 取

$$\begin{aligned}a'&=(f-b^2)/a,\\ b'&\equiv-b\mod a',\quad \deg b'<\deg a'.\end{aligned}\tag{16.4}$$

我们将在下节证明 $\mathrm{div}\ (a',b')\sim\mathrm{div}\ (a,b)$. 设 $\deg a=m$, $\deg b=n<m$, 则 $\deg a'=\max(2g+1,2n)-m$. 若 $m>g+1$, 则 $\deg a'\leqslant 2(m-1)-m=m-2$; 若 $m=g+1$, 则 $\deg a'=2g+1-(g+1)=g$. 当 $\mathrm{div}\ (a,b)$ 不是既约形式时, 可以重复利用上述方法, 得到一个与它线性等价的既约除子. 这实际上是 Guass 计算二次型既约形式的方法. 关于计算既约形式的改进算法可见文献 [47, 48].

设 C 为有限域 $\mathbb{F}_q$ 上由方程 $y^2 = f(x)$ 定义的超椭圆曲线. 类似基于椭圆曲线的公钥密码, 可以建立基于 C 的 Jacobian $J(\mathbb{F}_q)$ 上的公钥密码 (事实上, 椭圆曲线即是亏格 $g = 1$ 的超椭圆曲线, 椭圆曲线的点生成的群是与它的 Jacobian 同构的).

选取一个除子 $D \in J(\mathbb{F}_q)$, 要求 D 的阶是一个大素数. 每个用户选取私钥 k, 将 $D' = kD$ 作为该用户的公钥. 由于 $D' = \mathrm{div}\,(a', b')$, 多项式 a' 和 b' 的系数即可作为公钥使用. 利用下述方法, 可以在 $J(\mathbb{F}_q)$ 中随机选取一个基点 D. 设正整数 $m \leqslant g$, 随机选取 $\alpha \in \mathbb{F}_{q^m}$, 当 $f(\alpha)$ 为 $\mathbb{F}_{q^m}$ 中的平方元 (此情形发生的概率为 50%) 时, 计算 $f(\alpha)$ 的平方根 β, 则 $Q = (\alpha, \beta) \in \mathcal{C}$. 这时

$$D = \sum_{\sigma \in \mathrm{Gal}(F_{q^m}/\mathbb{F}_q)} Q^{\sigma} - m\mathcal{O}$$

为 $J(\mathbb{F}_q)$ 中的除子. 在计算 $D' = kD$ 时, 需要用到前面的算法.

已知 $D_1, D_2 \in J(\mathbb{F}_q)$, 且 $D_1 \in \langle D_2 \rangle$, 计算 m, 使得 $D_1 \sim mD_2$, 这就是超椭圆曲线上的离散对数问题 (HECDLP). 基于超椭圆曲线的公钥密码的安全性是建立在计算 HECDLP 的复杂度之上, 在前面介绍的小步 - 大步法和袋鼠法等一般的计算 DLP 的方法, 显然也适用于 HECDLP. FR 约化和 SSSA 约化也可推广到 HECDLP[48].

§16.2 虚 2 次代数函数域

方程 (16.1) 定义的超椭圆曲线 C 的函数域 $\overline{F}(C) = \overline{F}(x, y)$ 是有理函数域 $\overline{F}(x)$ 的 2 次扩域. 容易验证, $\overline{F}(C)$ 中的任一代数整函数一定形如 $a + by$, 其中 $a, b \in \overline{F}[x]$. 以 R 表示 $\overline{F}(C)$ 中所有代数整函数组成的环. $\overline{F}[x]$ 中所有素理想形如 $(x - \alpha)$ $(\alpha \in \overline{F})$, 它们在 R 中都分解为两个素理想 $\mathfrak{P}_1$ 和 $\mathfrak{P}_2$ 之积 ($\mathfrak{P}_1$ 与 $\mathfrak{P}_2$ 可以相同). 记 $\beta^2 = f(\alpha)$, 当 $f(\alpha) \neq 0$ 时, $(x - \alpha)$ 分解为 $\mathfrak{P}_1 = (x - \alpha, y - \beta)$ 和 $\mathfrak{P}_2 = (x - \alpha, y + \beta)$ 之积, 当 $f(\alpha) = 0$ 时, $(x - \alpha)$ 分解为 $(x - \alpha, y)^2$. 可见 C 上的有限点与 R 中的素理想一一对应. 进一步, $\mathcal{D}^{\circ}$ 中的除子 (仅考虑有限点部分) 与 R 的分式理想一一对应, 且两个除子之和对应的理想为它们各自对应的理想之积, 主除子对应主理想, 所以 C 的 Jacobi 与 R 的类群同构. 当 $D = \sum m_i Q_i - (\sum m_i)\mathcal{O}$ 为半既约除子时, D 对应 R 的一个理想 $\prod (x - \alpha_i, y - \beta_i)^{m_i}$, 其中 $Q_i = (\alpha_i, \beta_i)$.

设 $\mathfrak{R}$ 为 R 的一个整理想. 令

$$M = \{m(x) \in \overline{F}[x] \mid m(x) \in \mathfrak{R}\},$$

$$N = \{n(x) \in \overline{F}[x] \mid \exists m \in \overline{F}[x], 使得 m + ny \in \mathfrak{R}\},$$

M 和 N 都是 $\overline{F}[x]$ 中的主理想, 设 $M=(u)$, $N=(v)$, 则存在 $r+vy\in\mathfrak{R}$, 使得

$$\mathfrak{R}=(u,r+vy).$$

由于 $uy\in\mathfrak{R}$, 故 $v|u$, 又由于 $y(r+vy)=vf+ry\in\mathfrak{R}$, 故 $v|r$. 记 $u=av$, $r=bv$, 于是

$$\mathfrak{R}=v(a,b+y)\sim(a,b+y)$$

($\sim$ 表示理想的等价), 可以认为 $\deg b<\deg a$. 易见 $(b+y)(b-y)=b^2-f\in\mathfrak{R}\cap\overline{F}[x]$, 故 $a|b^2-f$. 记 $b^2-f=ac$, 由于 f 无重因子, 可见 $\gcd(a,b,c)=1$.

设 $\mathfrak{R}_i=(a_i,b_i+y)$, $\deg b_i<\deg a_i$, $b_i^2-f=a_ic_i$ $(i=1,2)$. 设 $\mathfrak{R}_1\mathfrak{R}_2\sim(a,b+y)$, $\deg b<\deg a$, $b^2-f=ac$, 现计算 a 和 b. 记 $\gcd(a_1,a_2,b_1+b_2)=d$, 则存在 $s_1,s_2,s_3\in\overline{F}[x]$, 使得 $d=s_1a_1+s_2a_2+s_3(b_1+b_2)$. 记 $a_1=a_1'd, a_2=a_2'd, b_1+b_2=hd$, 从而 $s_1a_1'+s_2a_2'+s_3h=1$. 由于 $b_1b_2+f=b_1b_2+b_i^2-a_ic_i=b_i(b_1+b_2)-a_ic_i$, 可见 $d\mid b_1b_2+f$. 我们有

$$\mathfrak{R}_1\mathfrak{R}_2=(a_1a_2,\ a_1(b_2+y),\ a_2(b_1+y),\ b_1b_2+f+(b_1+b_2)y).$$

显然

$$s_1a_1(b_2+y)+s_2a_2(b_1+y)+s_3(b_1b_2+f+(b_1+b_2)y)=d(b+y)\in\mathfrak{R}_1\mathfrak{R}_2,$$

其中

$$b=(s_1a_1b_2+s_2a_2b_1+s_3(b_1b_2+f))/d=s_1a_1'b_2+s_2a_2'b_1+s_3(b_1b_2+f)/d,$$

所以

$$\begin{aligned}\mathfrak{R}_1\mathfrak{R}_2&=\big(a_1a_2,\ a_1(b_2+y),\ a_2(b_1+y),\ b_1b_2+f+(b_1+b_2)y,\ d(b+y)\big)\\&=d\big(a_1'a_2'd,\ a_1'(b_2-b),\ a_2'(b_1-b),\ \frac{b_1b_2+f}{d}-hb,\ b+y\big).\end{aligned}$$

由于

$$\begin{aligned}b_2-b&=b_2(1-s_1a_1')-s_2a_2'b_1-s_3(b_1b_2+f)/d\\&=b_2(s_2a_2'+s_3h)-s_2a_2'b_1-s_3(b_2h-a_2'c_2)\\&=a_2'(b_2s_2-s_2b_1+s_3c_2),\end{aligned}$$

可见 $a_2'\mid b_2-b$, 同理 $a_1'\mid b_1-b$. 又

$$\begin{aligned}\frac{b_1b_2+f}{d}-hb&=\frac{b_1b_2+f}{d}(s_1a_1'+s_2a_2'+s_3h)\\&\quad-h\Big(s_1a_1'b_2+s_2a_2'b_1+s_3\frac{b_1b_2+f}{d}\Big)\\&=-a_1'a_2'(s_1c_2+s_2c_1).\end{aligned}$$

现在证明 $a_1'a_2' \in \mathfrak{R}_1\mathfrak{R}_2/d$. 由于 $da_1'a_2' \in \mathfrak{R}_1\mathfrak{R}_2/d$,

$$(b_1-b_2)a_1'a_2' = a_1'a_2'(b_1-b) - a_1'a_2'(b_2-b) \in \mathfrak{R}_1\mathfrak{R}_2/d,$$

$$c_1a_1'a_2' = \frac{b_1+b_2}{d}a_2'(b_1+y) - a_2'\Big(\frac{b_1b_2+f}{d} + \frac{b_1+b_2}{d}y\Big) \in \mathfrak{R}_1\mathfrak{R}_2/d,$$

故 $\gcd(d,\ c_1,\ b_1-b_2)\cdot a_1'a_2' \in \mathfrak{R}_1\mathfrak{R}_2/d$. 事实上 $\gcd(d,\ c_1,\ b_1-b_2)=1$, 否则若有不可约多项式 $p(x) \mid \gcd(d,\ c_1,\ b_1-b_2)$, 则 $p \mid a_1$, $p \mid c_1$, 由 $p \mid b_1+b_2$, $p \mid b_1-b_2$, 可得 $p \mid b_1$, 但 $\gcd(a_1,b_1,c_1)=1$, 这不可能. 所以我们证明了 $a_1'a_2' \in \mathfrak{R}_1\mathfrak{R}_2/d$. 最后得到

$$\mathfrak{R}_1\mathfrak{R}_2 \ \sim\ (a,\ b+y),$$

其中 $a = a_1'a_2'$. 可以设 $\deg b < \deg a$. 我们得到了 R 中两个理想类合成的算法, 也就是说 §16.1 中给出的 $\mathcal{C}$ 上的 Jacobian 中两个点相加的算法.

设 a' 和 b' 为 (16.4) 式所给, 由于

$$(a,\ b+y)\ \sim\ \big(a(b-y),\ b^2-y^2\big)\ \sim\ \big(c,\ -b+y\big)\ =\ \big(a',\ b'+y\big),$$

所以 $\mathrm{div}\ (a,b) = \mathrm{div}\ (a',b')$.

§16.3　小亏格超椭圆曲线离散对数的指标计算方法

设 $\mathcal{C}$ 是 $\mathbb{F}_q$ 上一条亏格 g 的超椭圆曲线, 即 $\mathcal{C}$ 是由如下方程定义的光滑仿射曲线:

$$\mathcal{C}:\ y^2+h(x)y=f(x),\quad \deg(f)=2g+1, \deg(h)\leqslant g.$$

记 J_q 是 $\mathcal{C}$ 的 Jacobian, 即

$$J_q := \mathrm{Jac}(\mathcal{C})(\mathbb{F}_q).$$

所谓超椭圆曲线离散对数问题, 是指下述问题：给定 $D_1, D_2 \in J_q$, 使得 $D_2 \in \langle D_1\rangle$, 即 D_2 属于由 D_1 生成的循环群, 则对于 (D_1, D_2) 的超椭圆曲线离散对数问题, 是指计算出最小正整数 $\lambda \in \mathbb{N}$, 使得 $D_2 = \lambda D_1$.

由前面可知 $\mathrm{Jac}(\mathcal{C})$ 的每一个点都可以惟一地表为一个既约除子, 即如下形式的除子:

$$\sum_{i=1}^{k} P_i - k\cdot\infty,$$

此处 P_i 是 $\mathcal{C}(\overline{\mathbb{F}}_q)$ 中的点, 且若 $i\neq j$, 则 $P_i \neq -P_j$, $k\leqslant g$, ∞ 是 $\mathcal{C}$ 上惟一的无穷远点, 于是以后将 $\mathrm{Jac}(\mathcal{C})$ 等同于既约除子的全体. 对于每一个既约除子 $D=\sum_{i=1}^{k}P_i -$

$k\cdot\infty$, $P_i=(x_i,y_i)$, 存在惟一的多项式对表示 $\{a(x),b(x)\}$, $a(x),b(x)\in\overline{\mathbb{F}}_q[x]$, 且

$$a(x)=\prod_{i=1}^{k}(x-x_i),$$

而 $b(x)$ 满足 $b(x_i)=y_i$, $\deg(b)<\deg(a)\leqslant g$ 且 $a(x)$ 整除 $b(x)^2+h(x)b(x)-f(x)$. J_q 中两个既约除子的和 (作为一个既约除子) 能够在 $O\big(g^2(\log q)^2\big)$ 个比特运算中计算出来.

而一个既约除子 $D=\{a(x),b(x)\}$ 是 J_q 中的点当且仅当 $a(x)$ 和 $b(x)$ 都在 $\mathbb{F}_q[x]$ 中.

为了应用指标计算法到超椭圆曲线离散对数问题, 我们需要有光滑性的概念. 令 $\mathfrak{P}$ 是 C 的 $\mathbb{F}_q$ 有理点集合, 即 $\mathfrak{P}=C(\mathbb{F}_q)$. 对任意 $P\in C(\overline{\mathbb{F}}_q)$, 置 $D(P)=P-\infty$.

定义 16.1 设 B 是 $\mathfrak{P}$ 的子集, 一个除子 D 称作相对于 B 光滑的, 如果它是既约的且 $D=\sum_{i=1}^{k}D(P_i)$, $P_i\in B\,(1\leqslant i\leqslant k)$. 而这个集合 B 称作一个因子基 (factor base). 一个除子称作潜在光滑的, 如果它相对于 $\mathfrak{P}$ 是光滑的.

定义 16.2 $\mathfrak{P}$ 中的一个点 P 称作相对于一个因子基 B 的大素因子, 如果 $P\notin B$. 一个既约除子 $D=\sum_{i=1}^{k}D(P_i)$ 称作几乎光滑的, 如果其中恰有一个 P_i 是大素因子, 其余的 P_j 都在因子基 B 中.

指标计算法还依赖于寻找光滑除子的一个拟随机游动, 叙述如下: 设 $R_0=\alpha_0D_1+\beta_0D_2$ 是该游动的起点. 注意 R_0 是由前面 §16.2 和 §16.3 中方法得出的既约除子 (α_0 和 β_0 是随机选取的整数). 设 $\mathcal{H}$ 是从群 $\langle D_1\rangle$ 到集合 $\{1,2,\cdots,m\}$ 的一个 Hash 函数. 对于 $1\leqslant j\leqslant m$, 计算随机除子

$$T^{(j)}=\alpha^{(j)}D_1+\beta^{(j)}D_2,$$

其中 $\alpha^{(j)}$ 和 $\beta^{(j)}$ 是随机选取的整数, 则除子的随机游动由下式给出:

$$R_{i+1}=R_i+T^{(\mathcal{H}(R_i))}.$$

在随机游动的每一步, 我们要计算出 α_{i+1} 和 β_{i+1} (mod $|D_1|$), 以及 R_{i+1}, 使得 $R_{i+1}=\alpha_{i+1}D_1+\beta_{i+1}D_2$, 其中 $|D_1|$ 表示 $\langle D_1\rangle$ 的阶. 如果 R_i 是一个光滑除子 (或几乎光滑除子), 则 α_i, β_i 和 R_i 将被存储起来.

我们知道, 经典的 ρ 方法是等待着随机游动发生一个碰撞 $R_{i_1}=R_{i_2}$, 从而得出离散对数 $\lambda=-(\alpha_{i_1}-\alpha_{i_2})/(\beta_{i_1}-\beta_{i_2})$ (mod $|D_1|$). 而对于指标计算法, 则需要利用光滑 (或几乎光滑) 除子.

从上述随机游动所获得的序列 $\{R_i\}$ 中, 找出其中光滑除子的子序列, 仍记为

$\{R_i\}$. 于是每一个 R_i 可写成

$$R_i = \alpha_i D_1 + \beta_i D_2, \qquad R_i = \sum_{j=1}^{k_i} D(P_{i,j}),$$

其中 $P_{i,j}$ 在因子基中, 而 $k_j \leqslant g$. 指标计算方法是利用 R_i 来获得一个形如 $\alpha D_1 + \beta D_2 = 0$ 的方程, 从而计算出 (D_1, D_2) 的离散对数. 为此, 将因子基 B 中元素排序为 $P_1, P_2, \cdots, P_{|B|}$. 对于每一个光滑除子

$$R_i = \sum_{j=1}^{k_i} D(P_{i,j}) = \sum_{l=1}^{|B|} a_{il} D(P_l)$$

对应一个向量

$$\overrightarrow{V_i} = (a_{i,1}, a_{i,2}, \cdots, a_{i,|B|}),$$

于是可以构造一个矩阵 $M = (a_{i,j})_{i,j}$, 其中每一行对应一个光滑除子. 而每一行中非零元素的个数最多为 g, 一旦 M 的尺度足够大, 以使得我们可以找到 M 的核中的一个非零向量, 则可以得出离散对数的值. 事实上, 一旦找到了方程组 $\vec{x}M = 0$ 的非零解, 则有

$$\sum_{i=0}^{m} \gamma_i \overrightarrow{V_i} = 0,$$

即

$$\sum_{i=0}^{m} \gamma_i R_i = 0.$$

将 $R_i = \alpha_i D_1 + \beta_i D_2$ 代入, 可得

$$\left(\sum_{i=0}^{m} \gamma_i \alpha_i\right) D_1 + \left(\sum_{i=0}^{m} \gamma_i \beta_i\right) D_2 = \alpha D_1 + \beta D_2 = 0. \tag{16.5}$$

从而可以得出 $D_2 = \lambda D_1$, $\lambda = -\alpha/\beta$(除非 $\beta = 0$, 此时, 必须重新开始给出随机游动的初始值, 再找出新的拟随机游动中的光滑除子并重复上述过程, 如果我们假定 $|D_1|$ 为素数, 则由随机性知出现在 $\beta = 0$ 的概率只有 $|D_1|^{-1}$, 故这种可能性是几乎不存在的 (因为 $|D_1|$ 很大).

由上面的分析, 可以给出以下算法:

(算法 16.1) Index_Calculus_I

输入: $\mathbb{F}_q$ 上亏格为 g 的曲线 $\mathcal{C}$ 的 $J_q = \mathrm{Jac}(\mathcal{C})(\mathbb{F}_q)$ 上一个除子 D_1, $|D_1| = n$ 为素数, 一个除子 $D_2 \in \langle D_1 \rangle$, 一个数 r.

输出: 一个正整数 λ, 使得 $D_2 = \lambda D_1$.

Step 1: 建立因子基 B. 对于每一个 $\mathbb{F}_q$ 上的一次首一不可约多项式 u_i, 试图找出 v_i, 使得 $\{u_i, v_i\}$ 是曲线的一个除子. 如果存在一个这样的 $\{u_i, v_i\}$, 将 $D_i = \{u_i, v_i\}$ 存储在 B 中. 一直做到 $|B| = q^r$.

Step 2: 随机游动的初始化. 对于 $1 \leqslant j \leqslant n$, 随机选取 $\alpha^{(j)}, \beta^{(j)} \in \{1, 2, \cdots, n\}$, 计算 $T^{(j)} := \alpha^{(j)} D_1 + \beta^{(j)} D_2$, 并随机选取 $\alpha_0, \beta_0 \in \{1, 2, \cdots, n\}$, 计算 $R_0 := \alpha_0 D_1 + \beta_0 D_2$, 置 $k = 1$.

Step 3: 主循环搜索

(a) 寻找潜在光滑除子. 计算

$$j = \mathcal{H}(R_0),\ R_0 := R_0 + T^{(j)},\ \alpha_0 := \alpha_0 + \alpha^{(j)} \pmod n,\ \beta_0 := \beta_0 + \beta^{(j)} \pmod n.$$

重复此步骤, 直到 $R_0 = \{u_0(z), v_0(z)\}$ 是一个潜在光滑除子.

(b) 潜在光滑除子的分解. 若 $u_0(z)$ 在 $\mathbb{F}_q$ 上分裂, 决定 $u_0(z)$ 的因子所对应的 $\mathcal{C}(\mathbb{F}_q)$ 中的点, R_0 是光滑的当且仅当 $u_0(z)$ 的因子全在 B 中, 若 R_0 是光滑的, 决定 $u_0(z)$ 的因子在因子基 B 中的位置, 并将结果存储为矩阵 $M = (a_{ij})$ 的一行. 将系数 $\alpha_k = \alpha_0$ 和 $\beta_k = \beta_0$ 存储. 若 $k < \#B + 1$, 置 $k := k + 1$, 并返回 Step 3(a).

Step 4: 找出在 Step 3 中获得的矩阵 M 的核中一个非零向量 $\gamma = (\gamma_k)$.

Step 5: 求解离散对数. 计算并输出

$$\lambda = -\left(\sum \alpha_k \gamma_k\right) / \left(\sum \beta_k \gamma_k\right) \pmod n$$

(如果分母为零, 则返回 Step 2).

下面考虑上述算法的时间复杂度.

Step 1: 为了选取我们的因子基, 考虑 $\mathcal{C}(\mathbb{F}_q)$ 中点的 x 坐标, 将 $\mathbb{F}_q$ 中元素排序成 $x_i \in \mathbb{F}_q$, $1 \leqslant i \leqslant q$, $x_1 = 0$, 计算方程

$$y^2 + h(X)y - f(X) = 0,\ \ X = x_i,$$

这显然可在 $O\big(g^2(\log q)^2\big)$ 个比特运算中完成. 然后在 $\mathbb{F}_q[y]$ 中分解该 2 次多项式, 这可在 $O\big(g^2(\log q)^2\big)$ 个比特运算中完成. 如果它在 $\mathbb{F}_q$ 中有根 $y_{i,1}$ 和 $y_{i,2}$, 将 $(x_i, y_{i,1})$ 和 $(x_i, y_{i,2})$ 存入 B 中, 对 $1 \leqslant i \leqslant q$ 重复此过程, 直到 $|B| = q^r$. 于是共要 $O(q)$ 次对 x 坐标的试探, 每次需要 $O\big(g^2(\log q)^2\big)$ 个比特运算, 故建立因子基的总计算量为 $O\big(g^2 q(\log q)^2\big)$ 个比特运算.

Step 2: 随机游动的初始化需要预计算除子 $T^{(i)}$, 对每一个 $T^{(i)}$, 我们在 $\{1, 2, \cdots, |J_q| - 1\}$ 中随机选取 $\alpha^{(i)}$ 和 $\beta^{(i)}$, 并置 $T^{(i)} = \alpha^{(i)} D_1 + \beta^{(i)} D_2$, 于是为了计算每一

个 $T^{(i)}$, 需要 $O(g\log q)$ 个 Jacobian 中的运算. 而每一个 Jacobian 中的运算需要 $O(g^2(\log q)^2)$ 个比特运算. 在实际中, 取 $m = O(\log(|J_q|)) = O(g\log q)$, 从而总的运算量为 $O(g^4(\log q)^4)$ 个比特运算.

为了计算 Step 3 中的运算量, 需要知道光滑除子在全体除子中所占的比例.

定理 16.1 设 $\frac{2}{3} < r < 1$, $q > (g-1)!$, J_q 中相对于因子基 B 的光滑除子的数目为

$$\frac{q^{rg}}{g!} + O\left(\frac{g^2 q^{r(g-1)}}{g!}\right).$$

证明 由定义, 相对于 B 的光滑除子一定可写成如下形式:

$$\sum_{i=1}^{k} D(P_i), \quad P_i \in B \text{且} \, k \leqslant g.$$

为了计算光滑除子的数目, 需要考虑在该表示中出现不同的 P_i 的除子的数目. 具有 g 个不同的 P_i 的光滑除子的数目为

$$\frac{1}{g!}\prod_{i=0}^{g-1}(q^r - i) = \frac{q^{rg}}{g!} - \frac{q^{r(g-1)}}{2(g-2)!} + O(q^{r(g-2)}).$$

这里应用了以下事实: P_1 可取 B 中任意一个元素, 故共有 $|B| = q^r$ 种取法, 一旦 P_1 取定, 则 P_2 可取 $B \setminus \{P_1\}$ 中任意元素, 从而有 $|B| - 1 = q^r - 1$ 种取法, $\cdots$, 故 $P_1, \cdots, P_g$ 全体的取法有 $\prod_{i=0}^{g-1}(q^r - i)$ 种, 但不同次序的 P_i 给出同一个除子 $\sum_{i=1}^{k} D(P_i)$, 从而具有 g 个不同的 P_i 的光滑除子的数目为 $\frac{1}{g!}\sum_{i=0}^{g-1}(q^r - i)$. 类似地, 具有 $g-1$ 个不同的 P_i 而另一个是重复的光滑除子的数目为

$$\frac{g-1}{(g-1)!}\prod_{i=0}^{g-2}(q^r - i) = \frac{q^{r(g-1)}}{(g-2)!} + O(q^{r(g-2)}),$$

而具有 $g-1$ 个不同的 P_i, 没有一个重复的光滑除子的数目为

$$\frac{1}{(g-1)!}\prod_{i=0}^{g-2}(q^r - i) = \frac{q^{r(g-1)}}{(g-1)!} + O(q^{r(g-2)}).$$

最后, 具有少于 $g-1$ 个不同的 P_i 的光滑除子的数目为 $O(q^{r(g-2)})$, 于是相对于 B 的光滑除子的总数为

$$\frac{q^{rg}}{g!} + O\left(\frac{g^2 q^{r(g-1)}}{g!}\right).$$

这就完成了定理的证明.

由定理 16.1, J_q 中光滑除子所占的比例为

$$\frac{\frac{q^{rg}}{g!}+O(\frac{g^2q^{r(g-1)}}{g!})}{q^g+O\big(gq^{g-1/2}\big)}=\frac{q^{-(1-r)/g}}{g!}+O\bigg(\frac{g^2q^{-(1-r)g-r}}{g!}\bigg)+O\bigg(\frac{gq^{-(1-r)g-1/2}}{g!}\bigg).$$

于是, 为了找到一个光滑除子, 需要搜寻 $O\big(g!q^{(1-r)g}\big)$ 次 (期望搜寻成功的次数).

下面的定理则给出了潜在光滑除子的数量:

定理 16.2 设 $q>(g-1)!$, J_q 中潜在光滑除子的数目为

$$\frac{q^g}{g!}+O\bigg(\frac{g}{g!}q^{g-1/2}\bigg).$$

证明 相对于 $\mathfrak{P}$ 的所有光滑除子都能够表成以下形式:

$$\sum_{i=1}^{k}D(P_i),\quad P_i\in\mathfrak{P},\ k\leqslant g.$$

为了计算光滑除子的数目, 需要考虑在该表示中出现不同的 P_i 的除子的数目. 因为 $|\mathfrak{P}|=q+O\big(\sqrt{q}\big)$, 具有 g 个不同的 P_i 的潜在光滑除子的数目为

$$\frac{1}{g!}\sum_{i=0}^{g-1}\big(|\mathfrak{P}|-i\big)=\frac{q^g}{g!}+O\bigg(\frac{g}{g!}q^{g-1/2}\bigg).$$

而具有少于 g 个不同的 P_i 的潜在光滑除子的数目为 $O(q^{g-1})$, 从而潜在光滑除子总数为

$$\frac{q^g}{g!}+O\bigg(\frac{g}{g!}q^{g-1/2}\bigg).$$

这就完成了定理的证明.

由定理 16.2 知 J_q 中潜在光滑除子所占的比例为

$$\frac{\frac{q^g}{g!}+O(\frac{g}{g!}q^{q-1/2})}{q^g+O(gq^{g-1/2})}=\frac{1}{g!}+O\bigg(\frac{g}{g!q^{1/2}}\bigg),$$

于是, 通过搜寻 $O(g!)$ 次, 我们期望能找到一个潜在光滑除子.

定理 16.3 设 $\frac{2}{3}<r<1$, $q>(g-1)!$, 在 J_q 中存在

$$\frac{q^{rg+1-r}}{(g-1)!}+O\bigg(\frac{q^{rg}}{(g-1)!}\bigg)$$

个几乎光滑除子.

证明 每一个几乎光滑除子都可表示为以下形式:

$$D(P)+\sum_{i=1}^{k-1}D(P_i),\ \ P\in\mathfrak{P}\setminus B,\ P_i\in B,\ k\leqslant g,$$

因此, 每一个几乎光滑除子都伴随到一个大素因子和最多 $g-1$ 个 $P_i\in B$. 与定理 16.1 的证明类似, 我们得到

$$\frac{q^{r(g-1)}}{(g-1)!}+O\Big(\frac{(g-1)^2q^{r(g-2)}}{(g-1)!}\Big)$$

个 $P_i\in B$ 可能的选取, 而对于大素因子而言, 存在 $|\mathfrak{P}|-|B|=q-q^r+O(\sqrt{q})$ 种可能的选取. 于是相对于 B 的几乎光滑除子的数目为

$$\begin{aligned}&\Big(\frac{q^{r(g-1)}}{(g-1)!}+O\Big(\frac{(g-1)^2q^{r(g-2)}}{(g-1)!}\Big)\Big)\Big(q-q^r+O(\sqrt{q})\Big)\\ =&\frac{q^{rg+1-r}}{(g-1)!}-\frac{q^{rg}}{(g-1)!}+O\Big(\frac{(g-1)q^{rg+1-2r}}{(g-2)!}\Big)+O\Big(\frac{q^{rg+\frac{1}{2}-r}}{(g-1)!}\Big)\\ =&\frac{q^{rg+1-r}}{(g-1)!}+O\Big(\frac{q^{rg}}{(g-1)!}\Big).\end{aligned}$$

在最后一个等式中, 我们用到了下述事实: $\frac{2}{3}<r<1$, $q>(g-1)!$, 这就完成了定理的证明.

Step 3: 分析 Step 3 的运算量. 为了保证 Step 4 中线性方程组的非零解的存在性, 我们需要找到 $O(|B|)=O(q^r)$ 个光滑除子. 而由定理 16.1 后面的分析, 为了找到这样的一个光滑除子, 需要的期望次数是 $O\big(g!q^{g(1-r)}\big)$, 从而在 Step 3 中, 随机游动的期望步数为

$$O(g^r)O\big(g!q^{g(1-r)}\big)=O\big(g!q^{g(1-r)+r}\big).$$

而在每一步的随机游动中, 首先要计算 R_i, 它需要 J_q 中一个加法和两个模 n 的加法, 这需要 $O\big(g^2(\log q)^2\big)$ 个比特运算. 对于 $R_i=\{a(x),b(x)\}$, 可以通过检查 $a(x)$ 在 $\mathbb{F}_q$ 上是否可分解成线性因子来判定 R_i 的潜在光滑性. 这可在 $O\big(g^2(\log q)^2\big)$ 个比特运算中完成, 因此整个 Step 3 (a) 的计算量为

$$O\big(g^2(\log q)^2\big)O\big(g!q^{g(1-r)+r}\big)=O\big(g^2g!q^{g(1-r)+r}(\log q)^2\big)$$

个比特运算.

现在考虑 Step 3 (b) 中完全分解一个潜在光滑除子所需要的计算量. 最简单的办法就是试除法, 这总共需要试除 $O(q)$ 次, 而每次试除所需比特运算量为 $O\big(g^2(\log q)^2\big)$ (这是因为 $a(x)$ 的次数为 $O(g)$), 从而完全分解一个潜在光滑除子所

需计算量为 $O\big(qg^2(\log q)^2\big)$ 个比特运算. 如果要检测一个除子是否为光滑除子, 则要做的试除只有 $O(q^r)$ 次 (这是因为因子基 B 的元素个数为 q^r), 于是判别一个潜在光滑除子是否为光滑除子并 (如果是光滑的) 用因子基 B 表示出来所需比特运算量为

$$O(q^r)O\big(g^2(\log q)^2\big) = O\big(q^r g^2(\log q)^2\big).$$

而我们需要对 $O(q^r)$ 个光滑除子进行上述完全分解, 故 Step 3 (b) 的计算量为 $O\big(q^{2r}g^2(\log q)^2\big)$ 个比特运算.

Step 4 的运算量估计: 矩阵 M 的尺度为 $O(q^r)\times O(q^r)$, 而 M 的每一行的重量 (即非零元的个数) 为 $O(g)$(事实上, 不大于 g), 于是 M 是一个重量为 $O\big(gq^r\big)$ 的稀疏矩阵. 因为 M 是稀疏的, 故可以应用文献 [49, 50] 中的算法, 来求解我们的线性方程组. 于是可以在 $O\big(gq^{2r}\big)$ 个模 $|J_q|$ 的运算中求得矩阵 M 的核中一个非零向量. 因为 $|J_q| = q^g + O\big(gq^{g-1/2}\big)$, 于是所需比特运算量为

$$O\big(gq^{2r}\big)\cdot O\big((g\log q)^2\big) = O\big(g^3q^{2r}(\log q)^2\big).$$

Step 5 的运算量估计: 设 $\gamma=(\gamma_k)$ 是 Step 4 求出的非零向量, 于是, 由 (16.5) 式, 有

$$\lambda = -\alpha/\beta \pmod{|J_1|},$$
$$\alpha = \sum_i \gamma_i\alpha_i, \quad \beta = \sum_i \gamma_i\beta_i,$$

其中 α_i 和 β_i 来自表达式 $R_i = \alpha_i D_1 + \beta_i D_2$($R_i$ 是用来建立我们的 M 的第 i 个除子). 计算 α 和 β 需要 $O(q^r)$ 个模 $|J_q|$ 运算, 而每一个模运算需 $O\big(g^2(\log q)^2\big)$ 个比特运算, 故 Step 5 总的比特运算量为 $O\big(g^2q^r(\log q)^2\big)$. 由以上分析, 我们可以得出下述定理:

定理 16.4 设亏格 $g\geqslant 3$, 则可以选取因子基 B, 使得算法 Index_Calculus_I 的运算量为 $O\big(g^5q^{2-\frac{2}{g+1}+\varepsilon}\big)$.

证明 从前面的分析, 算法 Index-Calculus-I 的各个步骤的运算量分别为

Step 1: $O\big(g^2q(\log q)^2\big)$,

Step 2: $O\big(g^4(\log q)^4\big)$,

Step 3 (a): $O\big(g^2g!q^{g(1-r)+r}(\log q)^2\big)$,

Step 3 (b): $O\big(q^{2r}g^2(\log q)^2\big)$,

Step 4: $O\big(g^3q^{2r}(\log q)^2\big)$,

Step 5: $O\big(g^2q^r(\log q)^2\big)$.

由于当 $\frac{2}{3} < r < 1$ 时, Step 1, 2, 3(b) 和 5 的运算量小于 Step 3(a) 和 Step 4, 故算法的总计算量为

$$O\big(g^2 g! q^{r+g(1-r)} (\log q)^2\big) + O\big(g^3 q^{2r} (\log q)^2\big).$$

为了使之最小化, 我们选取 r, 使得二者具有相同的量级, 即使得

$$(g-1)! q^{r+g(1-r)} = q^{2r}.$$

由此可算出

$$r = \frac{g + \log_q\big((g-1)!\big)}{g+1}. \tag{16.6}$$

由于 $q > (g-1)!$, 故 $0 < \log_q\big((g-1)!\big) < 1$, 从而

$$\frac{g}{g+1} < r < 1.$$

当 $g \geqslant 3$ 时, 有 $r > g/(g+1) > 2/3$. 于是当 r 按 (16.2) 式选取时, 总的计算量为

$$O\big(g^3 \big((g-1)!\big)^{\frac{2}{g+1}} q^{\frac{2g}{g+1}} (\log q)^2\big).$$

最后, 因 $g \geqslant 3$, 有 $(g/4)^{g+1} < (g-1)! < g^{g+1}$, 故总的计算量为

$$O\big(g^5 q^{2-\frac{2}{g+1}+\varepsilon}\big).$$

这就完成了定理 16.4 的证明.

为了给出指标计算方法的改进, 我们模仿数域筛法中大素数的应用, 然后再适当选取因子基的大小, 使得解线性方程组的运算量和搜寻光滑除子之间达到最佳平衡. 但是我们现在需要进一步利用 $\mathfrak{P}$ 中非因子基的那一部分点.

下面假定 $q > (g-1)!/g$ 且因子基具有尺度大小 $|B| = q^r$, 其中 $\frac{2}{3} < r < 1$.

为了应用几乎光滑除子, 我们将按它们在搜索步骤中出现的先后给其排序.

定义 16.3 设 R_i 是一个几乎光滑除子, 其大素因子为 P. 如果 R_i 之前的某个 $R_j\,(j < i)$ 的大素因子为 $\pm P$, 则称 R_i 是一个交除子.

若两个几乎光滑除子 R_1 和 R_2 具有大素因子 P, 即

$$R_1 = D(P) + \sum_{i=1}^{k_1-1} D(P_{1,i}), \quad R_2 = D(P) + \sum_{i=1}^{k_2-1} D(P_{2,i}), \qquad P_{1,i}, P_{2,i} \in B,$$

考虑

$$R_1 - R_2 = \sum_{i=1}^{k_1-1} D(P_{1,i}) - \sum_{i=1}^{k_2-1} D(P_{2,i}) := R'$$

(若 $P_{1,i} = P_{2,j}$(对某些 i, j), 则将它们消去). 若两个几乎光滑除子 R_1 和 R_2 具有的大素因子分别为 P 和 $-P$, 则考虑 $R_1 + R_2$, 与上面类似, 有

$$R_1 + R_2 = \sum_{i=1}^{k_1-1} D(P_{1,i}) + \sum_{i=1}^{k_2-1} D(P_{2,i}) := R', \qquad P_{1,i}, P_{2,i} \in B$$

(若某些 $P_{1,i} = -P_{2,j}$, 则将它们消去).

在两种情形下, R' 都分解为因子基中的除子之和. 但 R' 可能不是光滑的 (因 R' 可能不是既约的), 而伴随到 R' 的向量则可以和两个具有一个公共的 $P_i \in B$ 的光滑除子的差一样工作, 且 R' 的重量小于 $2g$.

设 P 是一个大素因子, 设有 $k(>1)$ 个几乎光滑除子具有大素因子 $\pm P$, 且这 k 个除子都出现在我们的随机游动中, 设为 $R_{j_1}, R_{j_2}, \cdots, R_{j_k}$, 其中 $k-1$ 个是交除子. 应用构造矩阵 M 时同样想法, 伴随 R'_{j_i} 到向量 $\boldsymbol{V}'_i$, 但 $\boldsymbol{V}'_i$ 中对应到 $D(P)$ 的坐标为 0, 从而得出 $k-1$ 个向量 $\boldsymbol{V}'_2, \cdots, \boldsymbol{V}'_k$, 它们对应于 $D(P)$ 的坐标都是 0. 显然有

$$\operatorname{span}\{\boldsymbol{V}_1, \cdots, \boldsymbol{V}_k\} = \operatorname{span}\{\boldsymbol{V}_1, \boldsymbol{V}'_2, \cdots, \boldsymbol{V}'_k\}.$$

一旦 R_{j_1} 被用来消去在 R_{j_i} 中的大素因子, 则用另一个 R_{j_l} 再做消去时, 对线性方程组而言不会产生任何新的信息. 我们用这些 $\boldsymbol{V}'_i$ 来构造矩阵 M.

为了以后分析方便, 我们假定 $\mathfrak{P}$ 中任意点 P_i 如果满足 $P_i = -P_i$, 则 P_i 在因子基中, 并且假定一个点 P 在因子基中当且仅当其对称点 $-P$ 也在因子基中. 注意这并不会增加计算量, 但可以简化分析. 下面给出改进的指标计算方法并分析其计算复杂度:

(算法 16.2) Index_Calculus_II

输入: $\mathbb{F}_q$ 上亏格为 g 的曲线 $\mathcal{C}$ 的 $J_q = \mathrm{Jac}(\mathcal{C})(\mathbb{F}_q)$ 上一个除子 D_1, $|D_1| = n$ 为素数, 一个除子 $D_2 \in \langle D_1 \rangle$, 一个数 r.

输出: 一个正整数 λ, 使得 $D_2 = \lambda D_1$.

(以下步骤, 除了下面的 Step 3(c) 外, 都与 Index_Calculus_I 中相应步骤完全相同)

Step 1: 建立因子基 B;

Step 2: 随机游动的初始化;

Step 3: 主循环搜索

(a) 寻找潜在光滑除子;

(b) 潜在光滑除子的分解. 若 $u_0(z)$ 在 $\mathbb{F}_q$ 上分裂, 决定 $u_0(z)$ 的因子所对应的 $\mathcal{C}(\mathbb{F}_q)$ 中的点;

(c) 若除子 R_0 是几乎光滑的, 检查它是否为一个交除子. 若不是, 将其加入非交除子列表. 若是, 消去其大素因子并将所得结果像光滑除子一样对待, 从而构造出矩阵 M;

Step 4: 同 Index_Calculus_I 中的 Step 4;

Step 5: 同 Index_Calculus_I 中的 Step 5.

为了分析上述算法的计算复杂度, 需要知道从几乎光滑除子能得出多少个方程. 为此, 需要估计有关交除子的数目.

设 $Q(n,s,i)$ 是如下事件的概率：从 n 个元素的集合中, 进行 s 次可重复抽样, 其中有 i 个交除子. 而令 $E_{n,s}$ 是交除子的期望数, 即

$$E_{n,s}=\sum_{i=1}^{s-1} iQ(n,s,i).$$

定理 16.5　若 $3\leqslant s<n/2$, 则

$$\frac{2s^2}{3n}<E_{n,s}<\frac{s^2}{n}.$$

证明　考虑在进行 $s+1$ 次可重复抽样后, 其中有 i 个交除子的概率 $Q(n,s+1,i)$, 则不难看出

$$Q(n,s+1,i)=\frac{n-2(s-i)}{n}Q(n,s,i)+\frac{2(s-i+1)}{n}Q(n,s,i-1),$$

这是因为, 若 T_{s+1} 含有大素因子 P_{s+1}, 则 T_{s+1} 是一个交除子当且仅当 $\pm P_{s+1}$ 出现在前 s 个几乎光滑除子中的 $s-i$ 个或 $s-i+1$ 个非交除子之一中, 从而

$$\begin{aligned}
E_{n,s+1}&=\sum_{i=0}^{s} iQ(n,s+1,i)\\
&=\sum_{i=0}^{s} i\left(\frac{n-2(s-i)}{n}Q(n,s,i)+\frac{2(s-i+1)}{n}Q(n,s,i-1)\right)\\
&=\sum_{i=0}^{s} i\frac{n-2(s-i)}{n}Q(n,s,i)+\sum_{i=1}^{s} i\frac{2(s-i+1)}{n}Q(n,s,i-1)\\
&=\frac{n-2s}{n}\sum_{i=0}^{s} iQ(n,s,i)+\frac{2}{n}\sum_{i=0}^{s-1} i^2Q(n,s,i)+\frac{2s}{n}\sum_{i=1}^{s} Q(n,s,i-1)\\
&\quad+\frac{2s-2}{n}\sum_{i=1}^{s}(i-1)Q(n,s,i-1)-\frac{2}{n}\sum_{i=1}^{s}(i-1)^2Q(n,s,i-1)
\end{aligned}$$

$$= \frac{n-2}{n}\sum_{i=0}^{s-1} iQ(n,s,i) + \frac{2s}{n}\sum_{i=0}^{s-1} Q(n,s,i)$$
$$= \frac{n-2}{n}E_{n,s} + \frac{2s}{n}.$$

由此递归关系式及 $E_{n,1}=0$, 有

$$E_{n,s} = \frac{n}{2}\left(1-\frac{2}{n}\right)^s + s - \frac{n}{2} = \frac{n}{2}\sum_{i=2}^{s}\binom{s}{i}\left(\frac{-2}{n}\right)^i.$$

因为 $\frac{2(s-i)}{in} < 1$, 上述和式中的项的绝对值是严格递减的. 于是

$$E_{n,s} < \frac{s(s-1)}{n} < \frac{s^2}{n}$$

且

$$E_{n,s} > \frac{s(s-1)}{n} - \frac{2s(s-1)(s-2)}{3n^2} > \frac{s^2}{n} - \frac{2s^3}{3n^2}$$
$$= \frac{s^2}{n}\left(1-\frac{2s}{3n}\right) > \frac{2s^2}{3n}.$$

这就证明了定理.

我们来分析 Index_Calculus_II 的计算复杂度. 由于除了 Step 3 外, 其余步骤与 Index_Calculus_II 完全一样, 故只要分析 Step 3 的搜寻的运算量.

令 n 是大素数的数目, 则 $n = \#\mathcal{C}(\mathbb{F}_q) - |B| = q - q^r + O(\sqrt{q})$. 由于我们期望能搜寻到足够多的交除子以建立矩阵 M 且使 M 的核非零, 故期望次数 $E_{n,s} = O(q^r)$, 但由定理 16.5, $E_{n,s} = O(s^2/n)$, 故有 $s = O(q^{\frac{r+1}{2}})$. 于是为建立所需线性方程组, 将花费

$$O\left(s(g-1)!q^{(g-1)(1-r)}\right) = O\left((g-1)!q^{(g-1)(1-r)+\frac{r+1}{2}}\right)$$

步随机游动. 这里用到了以下事实: 在 J_q 中的几乎光滑除子所占比例为 (定理 16.3)

$$\frac{\frac{q^{rg+1-r}}{(g-1)!} + O\left(\frac{q^{rg}}{(g-1)!}\right)}{q^g + O(gq^{g-1/2})} = \frac{q^{-(1-r)(g-1)}}{(g-1)!} + O\left(\frac{q^{-(1-r)g}}{(g-1)!}\right) + O\left(g\frac{q^{-(1-r)(g-1)-1/2}}{(g-1)!}\right),$$

从而为找出一个几乎光滑除子所需要搜寻的期望次数为

$$O\left((g-1)!q^{(1-r)(g-1)}\right).$$

而由定理 16.1 后的讨论, 平均 $O(g!q^{(1-r)g})$ 次搜寻中产生一个光滑除子, 故在

$$O\left((g-1)!q^{(g-1)(1-r)+\frac{r+1}{2}}\right)$$

次随机游动中能产生出

$$\frac{O\big((g-1)!q^{g-rg+r-1+\frac{r+1}{2}}\big)}{O\big(g!q^{(1-r)g}\big)}=O\Big(\frac{1}{g}q^{r-\frac{1-r}{2}}\Big)$$

个光滑除子. 这些光滑除子当然可能用来获得一些线性方程组, 但这对运算时间的影响并不是非常大.

正如 Index_Calculus_I 中类似, 计算 $R_i=\{a(x),b(x)\}$, α_i,β_i 以及检查 R_i 是否为几乎光滑的需要 $O\big(g^2(\log q)^2\big)$ 比特运算, 从而整个 Step 3 (a) 需要

$$O\big(gg!q^{(g-1)(1-r)+\frac{r+1}{2}}(\log q)^2\big)$$

个比特运算. 因为在每 $O(g!)$ 个除子中有一个是几乎光滑的, 可期望在搜寻过程中找到

$$\frac{O\big((g-1)!q^{g-rg+-1+\frac{r+1}{2}}\big)}{O(g!)}=O\Big(\frac{q^{(g-1)(1-r)+\frac{r+1}{2}}}{g}\Big)$$

个潜在光滑除子. 对每一个潜在光滑除子, 计算在 R_i 的表示中对应于 $\mathfrak{P}$ 中的点, 这需要 $O(g^2(\log q)^2)$ 个比特运算, 然后检查它是否光滑, 还是几乎光滑. 若是光滑的, 用它来产生一个线性方程, 若是几乎光滑的, 则查看它前面的几乎光滑除子, 看它是否为一个交除子, 这需要 $O(\frac{1+r}{2}\log q)$ 个比特运算 (这是因为存在 $O(q^{\frac{1+r}{2}})$ 个非交除子, 并且在做搜寻时只有大素因子需要考虑), 如果有一个交除子, 则可以消去其大素因子, 从而可应用消去大素因子后的除子来增加一个线性方程, 否则将该除子加在非交除子的列表中. 这个过程期望在

$$O\big(gq^{(g-1)(1-r)+\frac{1+r}{2}}(\log q)^2\big)$$

个比特运算内 (对在该搜寻中碰到的所有潜在光滑除子) 完成.

从而 Index_Calculus_II 中整个搜寻过程可在 $O\big(gg!q^{(g-1)(1-r)+\frac{1+r}{2}}(\log q)^2\big)$ 个比特运算中完成.

定理 16.6 设亏格 $g\geqslant 3$, 则可以选取因子基 B, 使得算法Index-Calculus-II的运算量为 $O\big(g^5q^{2-\frac{4}{2g+1}+\varepsilon}\big)$.

证明 由前面的讨论, 算法的各步骤运算量为

Step 1: $O\big(g^2q(\log q)^2\big)$,

Step 2: $O\big(g^4(\log q)^4\big)$,

Step 3: $O\big(gg!q^{(g-1)(1-r)+\frac{1+r}{2}}(\log q)^2\big)$,

Step 4: $O\big(g^3q^{2r}(\log q)^2\big)$,

Step 5: $O\big(g^2q^r(\log q)^2\big)$.

与定理 16.4 的证明类似, Step 3 和 Step 4 是最耗时的, 故整个算法复杂度为

$$O\big(gg!q^{(g-1)(1-r)+\frac{r+1}{2}}(\log q)^2\big)+O\big(g^3q^{2r}(\log q)^2\big).$$

为使之最小化, 令两者具有相同的量级, 故

$$(g-1)!q^{(g-1)(1-)+\frac{r+1}{2}}=gq^{2r},$$

从而

$$r=\frac{g-\frac{1}{2}+\log_q\big((g-1)!/g\big)}{g+\frac{1}{2}}.$$

因为 $g\geqslant 3$, 易知 $2/3<r<1$, 于是可知运算量为

$$O\big(g^3((g-1)!/g)^{\frac{4}{2g+1}}q^{\frac{4g-2}{2g+1}}(\log q)^2\big).$$

由于 $(g/4)^{g+1/2}<(g-1)!/g<g^{g+1/2}$ $(\forall g\geqslant 3)$, 故运算量为 $O\big(g^5q^{2-\frac{4}{g+1}+\varepsilon}\big)$, 定理证毕.

§16.4 大亏格超椭圆曲线离散对数的指标计算方法

本节讨论大亏格超椭圆曲线离散对数问题的指标计算方法. 为此, 需要给出更一般的光滑性概念.

定义 16.4 设 $D=\{u,v\}$ 是一个既约除子, D 称为素除子当且仅当多项式 u 是 $\mathbb{F}_q$ 上不可约的多项式.

不难看出以下事实:

定理 16.7 $\mathrm{Jac}(\mathcal{C})$ 的一个除子 $D=\{u,v\}$ 可以写成一些素除子 $\{u_i,v_i\}$ 之和, 其中 u_i 是 u 的素因子.

定义 16.5 设 $\mathcal{S}$ 是正整数, 一个除子称为是 $\mathcal{S}$ 光滑的, 如果它的素除子的次数最多为 $\mathcal{S}$(此处若 $\{u_i,v_i\}$ 是一个除子, 则称 $\deg(u_i)$ 是除子 $\{u_i,v_i\}$ 的次数). 特别地, 若 $\mathcal{S}=1$, 则一个 1 光滑除子是除子 $\{u,v\}$, 使得 u 在 $\mathbb{F}_q$ 上完全分裂.

每一个除子类均含有惟一的既约除子 $\{a,b\}$, 它对应于

$$K(\mathcal{C})=\mathbb{F}_q[X,Y]/(Y^2+hY-f)$$

的理想 $(a,Y-b)$, $a,b\in\mathbb{F}_q[X]$, $\deg b<\deg a\leqslant g$ 且 $a|b^2+bh-f$. 令 $\mathfrak{p}_{\mathcal{S}}$ 是所有次数不超过 $\mathcal{S}$ 的素除子的集合, $n_{\mathcal{S}}=\#\mathfrak{p}_{\mathcal{S}}$, 而 $n'_{\mathcal{S}}$ 是 $\mathrm{Jac}(\mathcal{C})$ 中所有次数不超过 $\mathcal{S}$ 的除子的集合. 置 $N=\#\mathrm{Jac}(\mathcal{C})$, $N'=q^g$, 任给除子 D, 则 D 的既约代表元可以在 N' 的多项式时间内计算出来. 而集合 $\mathfrak{p}_{\mathcal{S}}$ 则可如下构造出来: 首先列出所有次数不大于 $\mathcal{S}$ 的不可约多项式 $a\in\mathbb{F}_q[X]$, 然后解方程 $y_a^2+hy_a-f\equiv 0 \pmod a$, 这可以

利用概率多项式算法解决. 若此方程无解, 则是惰性的, 从而对应于 $K(\mathcal{C})$ 的素除子 $P=\operatorname{div}(a)$, 于是它将不出现在因子基中. 若方程有重根 b, 则 a 是分歧的; 它对应于 $K(\mathcal{C})$ 的惟一素除子 $P=\{a,b\}$, P 的次数为 $\deg(a)$, a 和 P 称为分歧的. 若方程有两个解 b 和 $-b-v\in\mathbb{F}_q[X]$, 则存在 $K(\mathcal{C})$ 中两个素除子 $P=\{a,b\}$, $\overline{P}=\{a,-b-v\}$, 其次数均为 $\deg(a)$, a 和 P 及 $\overline{P}$ 称为分裂的. 注意解 2 次方程可以在概率多项式时间内完成. 下面我们描述算法:

(算法 16.3) Index_Calculus_BigGenus

输入: 一个阶为 N 的循环群 G, g_1 为 G 的生成元, $g_2\in G$.

输出: 一个正整数 $l\in\{0,1,\cdots,N-1\}$, 使得 $g_2=lg_1$.

Step 1: 选取光滑性界 $\mathcal{S}$, 构造因子基 $\mathfrak{P}_{\mathcal{S}}=\{p_1,p_2,\cdots,p_n\}$, $n=n_{\mathcal{S}}$, 令 $k=\lceil\log_2 n+\log_2\log_2 N\rceil+1$;

Step 2: 构造矩阵 $A=\left(a_{ij}\right)\in\left(\mathbb{Z}/N\mathbb{Z}\right)^{n\times(2kn)}$ 如下: 对于 $j=1,2,\cdots,kn$, 随机选取 α_i, $\beta_j\in\mathbb{Z}/N\mathbb{Z}$, 直到 $\alpha_j g_1+\beta_j g_2$ 是 $\mathcal{S}$ 光滑的并写

$$\alpha_j g_1+\beta_j g_2=\sum_{i=1}^{n}a_{ij}p_i. \tag{16.7}$$

对于 $j=kn+1,\cdots,2kn$, 写 $j=(k+l)n+m$, $0\leqslant l\leqslant k-1$, $1\leqslant m\leqslant n$, 随机选取 $\alpha_j,\beta_j\in\mathbb{Z}/N\mathbb{Z}$, 直到 $\alpha_j g_1+\beta_j g_2-p_m$ 是 $\mathcal{S}$ 光滑的, 然后写

$$\alpha_j g_1+\beta_j g_2=p_m+\sum_{i=1}^{n}b_{ij}p_i=\sum_{i=1}^{n}a_{ij}p_i; \tag{16.8}$$

Step 3: 利用后面将给出的随机化过程, 试着找到一个非零向量 $\gamma=(\gamma_1,\cdots,\gamma_{2kn})\in\operatorname{Ker}(A)$, 如果这个过程失败, 则返回 Step 2;

Step 4: 若 $\sum_{j=1}^{2kn}\beta_j\gamma_j$ 在 $(\mathbb{Z}/N\mathbb{Z})$ 中可逆, 则输出

$$-\left(\sum_{j=1}^{2kn}\beta_j\gamma_j\right)^{-1}\left(\sum_{j=1}^{2kn}\alpha_j\gamma_j\right),$$

否则返回 Step 2.

如果上述算法在 Step 4 停止, 则它输出了正确的离散对数 $\log_{g_1}g_2$, $\gamma\in\operatorname{Ker}(A)$ 表明

$$0=\sum_{j=1}^{2kn}a_{ij}\gamma_j,\quad \forall i=1,2,\cdots,n,$$

将 p_i 乘上述这些方程并求和, 有

$$0=\sum_{j=1}^{2kn}\Big(\sum_{i=1}^{n}a_{ij}p_i\Big)\gamma_j=\Big(\sum_{j=1}^{2kn}\alpha_j\gamma_j\Big)g_1+\Big(\sum_{j=1}^{2kn}\beta_j\gamma_j\Big)g_2.$$

因为 g_1 和 g_2 都是 N-torsion 的, 两边乘上 $\sum_{j=1}^{2kn}\beta_j\gamma_j$ 在 $\mathbb{Z}/N\mathbb{Z}$ 中的逆 (如果存在), 就给出了正确的结果.

下面分析 Step 3 中的线性方程求解问题. 因为 $\operatorname{rank}(A)\leqslant n$, 总可以找到一个非零向量 $\gamma\in\operatorname{Ker}(A)$. 我们将充分利用矩阵 A 的稀疏结构, 其每一列仅有 $\widetilde{O}(1)$ 个非零元. 此处记号 $\widetilde{O}(f)$ 意义如下：对于 N' 的某个正函数 f, $\widetilde{O}(f)$ 记如下函数的集合：它们在相差一个 $\log N'$ 的幂次下, 在 $O(f)$ 中, 即

$$\widetilde{O}(f)=\{g\,|\,g\big(\log N'\big)^{\alpha}\in O(f), \text{对某个整数}\alpha\}.$$

为了利用矩阵的稀疏性, 可以应用一个随机化的 Lanczos 算法. 我们需要以下结论, 它可以由文献 [51] 中的定理 6.2 推出.

定理 16.8 *设 $\mathbb{F}_q$ 是 q 元域, $A\in\mathbb{F}_q^{n\times d}$ 是一个秩为 r 的矩阵, 有 ω 个非零元, 且 $b\in\mathbb{F}_q^n$, 则存在一个概率算法, 它给出一个向量 $x\in\mathbb{F}_q^d$, 使得 $Ax=b$, 或者算法失败, 整个算法复杂度为 $\mathbb{F}_q$ 中 $O\big(r(\omega+d)\big)$ 个运算, 而失败的概率最多为 $\frac{11d^2-d}{2(q-1)}$.*

更进一步, 通过将右边随机化, 此算法输出的解向量在所有可能的解中可以一致的变化：按照一个一致分布选取 $y\in\mathbb{F}_q^d$, 求解 $A\overline{x}=b+Ay$, 令 $x=\overline{x}-y$. 若 y 在 $\mathbb{F}_q^d/\operatorname{Ker}(A)$ 的一个固定的类上变化, 则 $\overline{x}$ 与 y 无关, 而 x 将在方程的解空间 $\overline{x}+\operatorname{Ker}(A)$ 上一致地分布. 因此, 相同的断言对 y 不属于一个固定的类也成立.

当 q 相比较于 d 较小的时候, 不能直接应用上述定理, 此时将问题转换到一个域扩张. 设 p 是 $\mathbb{F}_q$ 的特征, 令 $v=\min\{l: q^l>11d^2, p\nmid l\}$, $q'=q^v$, 则 $q^{v-2}\leqslant 11d^2$, 从而 $q'\in O(d^2q^2)$. 我们想求解一个 $\mathbb{F}_{q'}$ 上的矩阵方程并将所得解投影到 $Ax=b$ 的一个解 $x\in\mathbb{F}_q^d$ 上. 对于投影, 可以利用迹函数 $\operatorname{Tr}:\ \mathbb{F}_{q'}\to\mathbb{F}_q$, 它是一个 $\mathbb{F}_q$ 向量空间之间的同态, 且作用在 $\mathbb{F}_q$ 上为一个 v 数乘运算. 设 $b'=v'b\in\mathbb{F}_q^d$, $vv'\equiv 1 \pmod p$, 则 $vb'=b$. v' 的存在是由 $(v,p)=1$ 保证的, 而且 v' 可由扩充的欧几里德除法在 $O\big(\log v\log p\big)$ 时间内求得.

这些计算量以及 $v'b$ 的计算量相较于下面的线性代数步骤均可忽略不计. 利用 Eberly 和 Kaltofen 的算法求解 $Ax'=b'$, 这一步骤成功概率至少为 $1-\frac{11d^2-d}{2(q'-1)}\geqslant 1/2$. 令 $x=\operatorname{Tr}(x')$, 则从迹的线性性, 有

$$Ax=\operatorname{Tr}(Ax')=\operatorname{Tr}(b')=vb'=b.$$

更进一步, $Ax=b$ 的任何解 $x\in\mathbb{F}_q^d$ 均可由此法获得, 且它们均有相同的出现概率. 亦即对一个给定的解 x, 方程 $Ax'=b'$ 在 $\mathbb{F}_{q'}^d$ 上的解集中那些在迹函数下映到 x 的

解由 $v'x+(\mathrm{Ker}(A)\cap\mathrm{Ker}(\mathrm{Tr}))$ 给出，其个数

$$(q')^{\dim(\mathrm{Ker}(A)\cap\mathrm{Ker}(\mathrm{Tr}))}$$

与 x 无关. 因此, 我们证明了下面的结果：

定理 16.9　*设 $A\in\mathbb{F}_q^{n\times d}$ 是秩为 r 的矩阵, 有 ω 个非零元素, $b\in\mathbb{F}_q^n$, 则存在一个概率算法, 它或者输出一个向量 $x\in\mathbb{F}_q^d$, 使得 $Ax=b$, 或者失败. 算法的运算时间为 $O\big(r(\omega+d)\log^2(dq)\big)$, 而失败的概率最多为 1/2. 更进一步, 输出的向量在所有可能的解中是一致分布的.*

这就对 N 为素数的情形解决了线性代数步骤 Step 3, 否则, 我们分解 N, 并计算 $\gamma \bmod p^v$, $p^v\|N$, 然后利用中国剩余定理求得结果. 而模 p^v 的计算可以借助提升过程分解为 v 个模 p 的迭代过程：假设一个非零解 $\gamma_1\in\{0,1,\cdots,p^e-1\}^{2kn}$ 已经求得, 即

$$A\gamma_1\equiv 0 \pmod{p^e},$$

于是 $A\gamma_1=p^e\delta$, $\delta\in\mathbb{Z}^{2kn}$. 设存在 $Ax\equiv\delta \pmod p$ 的解 γ_2, 则 $p^e\gamma_2-\gamma_1$ 是 $Ax\equiv 0 \pmod{p^{e+1}}$ 的一个非零解. 若所有模去一个素数的计算在所有可能的解中输出一个一致分布的随机向量, 则组合出来的结果在 A 的核中也一致地变化.

然而, 通过考虑 A 的初等因子形式不难看出, 上述提升过程可能失败当且仅当 $\mathrm{rank}_{\mathbb{Q}}(A)\neq\mathrm{rand}_{\mathbb{Z}/p\mathbb{Z}}(A)$(因为此时矩阵方程 $Ax\equiv\delta \pmod p$ 不必有解). 这就是为什么我们要生成一个矩阵 A, 它的列数要比 $n+1$ 多得多. 我们需要下面的结果：

定理 16.10　*设 V 是域 $\mathbb{F}$ 上的向量空间, $\dim(V)=n<\infty$, 设 $\mathcal{S}$ 是 V 中向量的有限集合, $b_1,b_2,\cdots,b_n$ 是 V 的一组基. 令 $k\in\mathbb{N}$, 在 $\mathcal{S}$ 中以任意的概率分布做 $2kn$ 次独立取样, 将所取元素记为 $v_1,\cdots,v_{kn},w_1,\cdots,w_{kn}$, 记 V' 是 V 中由 $v_1,\cdots,v_{kn}$ 和 $b_j+w_{(j-1)k+i}(j=1,\cdots,n,i=1,2,\cdots,k)$ 生成的子空间, 则 $V=V'$ 的概率至少为 $1-\frac{n}{2^{k-1}}$.*

这个定理的证明可参见文献 [52].

将定理 16.10 应用到现在的情形：向量空间 V 是 $\mathbb{Z}/p\mathbb{Z}$ 上长度为 n 的列向量空间, V 的基是典范基, 集合 $\mathcal{S}$ 表示 G 中光滑元的所有列向量的集合. 于是生成 V' 的向量正好对应于形成矩阵 A 的向量, 因此, 在 $\mathbb{Z}/p\mathbb{Z}$ 上的提升可能的概率至少为 $1-\frac{n}{2^{k-1}}$. 最多存在 $\log_2 N/2$ 个不同的素数 p, 使得 $p^2|N$, 故对所有的 p 提升均成为可能的概率至少为 $1-\frac{n\log_2 N}{2^k}\geqslant 1/2$(由 k 的选取：$k=\lceil\log_2 n+\log_2\log_2 N\rceil+1$)。在此情形下, 将定理 16.9 中算法重复 $\log_2(2\log_2 N)$ 次, 我们获得模一个素数的一个问题的解的概率至少为 $1-\frac{1}{2^{\log_2(2\log_2 N)}}=1-\frac{1}{2\log_2 N}$. 而最多求解 $\log_2 N$ 个单个问题后, 我们将以至少 1/2 的概率获得一个模 N 的解答. 结合起来, Step 3 的成功概率至少为 1/4. 此情形下输出的向量在其核上是一致分布的.

为了估计算法中 Step 2 和 Step 4 中一个循环的成功概率, 先假定 Step 2 已经成功地完成. 先来估计 Step 4. 如上所述, Step 3 成功的概率至少为 1/4. 如果在 Step 4 中 $\sum_{j=1}^{2kn}\beta_j\gamma_j$ 在 $\mathbb{Z}/N\mathbb{Z}$ 中不可逆, 算法可以失败. 但这种事情出现的概率十分小, 对一个给定的 $j \leqslant kn$ 和任意 β_j, 因为 g_1 是 G 的生成元, α_j 是一致分布的, 元素 $\alpha_j g_1+\beta_j g_2$ 在全体群元素上是一致分布的. 相对结论对 $j>kn$ 和 $\alpha_j g_1+\beta_j g_2-p_m$ 亦成立, 因此, 矩阵 A 和向量 β 是独立的随机变量, 从而 γ 和 β 亦为独立的. 设 p 是 N 的一个素因子, 由于 γ 在全体核向量上一致分布, $\gamma \not\equiv 0 \pmod p$ 的概率至少为 $1-\frac{1}{p}$. 于是 $\gamma \bmod p$ 在 $\mathbb{Z}^{2kn}$ 中的正交空间的维数是 $2kn-1$, 且 $\beta \bmod p$ 不正交于 $\gamma \bmod p$ 的条件概率至少为 $1-\frac{1}{p}$, 因此 $\sum_{j=1}^{2kn}\beta_j\gamma_j$ 在 $\mathbb{Z}/N\mathbb{Z}$ 中可逆的概率至少为 $\prod_{p|N}(1-\frac{1}{p})^2=(\frac{\phi(N)}{N})^2$, 因而从 Step 2 到 Step 4 的一个循环的成功概率为 $O\big(1/(\log\log N)^2\big)$. 此处用到了事实 $\phi(N)/N \in O\big(1/\log\log N\big)$.

回顾 $n=n_{\mathcal{S}}=\#\mathfrak{P}_{\mathcal{S}}$, $n'=n'_{\mathcal{S}}$ 是次数不超过 $\mathcal{S}$ 的除子 $D=\{u,v\}$ 的个数. 记 $\mathcal{M}_{\mathcal{S}}=\big\{D=\{u,v\} \mid \deg(u)\leqslant\mathcal{S}\big\}$, 则 $n'=n'_{\mathcal{S}}=\#\mathcal{M}_{\mathcal{S}}$. 显然, $\mathcal{M}_{\mathcal{S}}$ 中元素全体可在 $\mathcal{S}$ 的多项式时间和 $n'_{\mathcal{S}}$ 的线性时间里列举出来. 而一个元素 m 是否为素除子可以在 $\deg(m)$ 的多项式时间和 $n'_{\deg(m)}$ 线性时间内测试出来 (这可通过对所有次数小于 $\deg(m)$ 的元素试除来进行), 因此 $\mathfrak{P}_{\mathcal{S}}$ 能够在 $\mathcal{S}$ 的多项式时间和 $n'_{\mathcal{S}}$ 的 2 次时间内构造出来, 即 $\mathfrak{P}_{\mathcal{S}}$ 可在 $\widetilde{O}(n'^2)$ 中构造出来.

现在记 $N_{\mathcal{S}}$ 是 G 中 $\mathcal{S}$ 光滑元素数目, 令 t_s 和 t_d 分别是一个光滑性测试和一个光滑元分解成素除子之和的期望时间的上界. 计算 g_1 和 g_2 的一个线性组合并测试其光滑性所需时间为 $\widetilde{O}(t_s)$, 这个过程的期望重复次数为 $N/N_{\mathcal{S}}$(以找到一个光滑元), 因此 Step 2 的总耗时为

$$\widetilde{O}\left(n\left(\frac{N}{N_{\mathcal{S}}}t_s+t_d\right)\right) \subseteq \widetilde{O}\left(n\frac{N}{N_{\mathcal{S}}}t_s+n^2\right),$$

因为 $2kn,\ t_d \in \widetilde{O}(n)$.

令 t_f 是分解 N 的时间, 正如前面分析的, 在 Step 3 中我们需要执行定理 16.9 中的算法 $\log_2(2\log_2 N)\log_2 N$ 次, 而 A 的每一列中非零元素个数是 $\widetilde{O}(1)$, 且 $\log_2(2\log_2 N)\log_2 N \in \widetilde{O}(1)$, 从而 Step 3 的耗时为 $\widetilde{O}(t_f+n^2)$.

最后, Step 4 可以在 $\widetilde{O}(n)$ 中完成. 因为平均而言, 从 Step 2 到 Step 4 只要重复 $O\big((\log\log N)^2\big)$ 次, 且 $n \leqslant n'$, $O\big((\log\log N)^2\big) \subseteq \widetilde{O}(1)$, 故算法的总计算量为

$$\widetilde{O}\left(t_f+n'^2+n'\frac{N}{N_{\mathcal{S}}}t_s\right). \tag{16.9}$$

下面分别考虑上式中各个量 $t_s, t_f, N_{\mathcal{S}}$. 先看 t_s, 由定义, t_s 是一个光滑性测试的时间之上界, 而由定义 16.4 和 16.5, 测试一个除子的光滑性, 归结到判断首一多项

式的光滑性. 更精确地说, 设 $D=\{f,g\}$ 是一个既约除子, 则测试 D 的 $\mathcal{S}$ 光滑性, 等价于判断 f 是否分解为一些不超过 $\mathcal{S}$ 次的不可约多项式之积. 令 $g=f/\gcd(f,f')$ 是 f 的无平方因子部分, 则 f 的光滑性等价于 g 的光滑性, 因为 $X^{q^i}-X$ 是 $\mathbb{F}_q[X]$ 上所有次数为 i 的首一不可约多项式之积, 故 g 是光滑的, 当且仅当

$$g=\operatorname{lcm}\big(\{\gcd(g,X^{q^i}-X)\,|\,i=1,2,\cdots,\mathcal{S}\}\big).$$

而这可以在 $\mathcal{S}$ 和 $\deg(f)$ 的多项式时间内完成, 但 $\deg(f)\leqslant g$, $N=O(q^g)$, 因此 $\deg(f)\in O(\log N)$, 于是 $t_s\in\widetilde{O}(1)$, 从而 Index_Calculus_BigGenus 的总运算量为

$$\widetilde{O}\left(t_f+n'^2+n'\frac{N}{N_{\mathcal{S}}}\right).$$

回忆一下亚指数函数的有关定义：设输出的尺度为 $\log N'$, 一个参数 $\alpha\in(0,1)$, $c>0$, 则记

$$L_{N'}(\alpha,c)=e^{c(\log N')^{\alpha}(\log\log N')^{1-\alpha}}.$$

显然, α 越小, 上述函数越接近于多项式 $L_{N'}(0,\lceil c\rceil)=\big(\log N'\big)^{\lceil c\rceil}$. 若 $\alpha=\frac{1}{2}$, 简记为 $L_{N'}(c):=L_{N'}(\frac{1}{2},c)$. 显然, 有以下简单的关系式：

$$L_{N'}(c_1)\cdot L_{N'}(c_2)=L_{N'}(c_1+c_2),$$

及

$$L_{N'}(c_1)+L_{N'}(c_2)\in O\big(L_{N'}(\max(c_1,c_2))\big).$$

更进一步, 显然有

$$\widetilde{O}(1)\subseteq L_{N'}\big(o(1)\big),\quad O\big(L_{N'}(\alpha,c)\big)\subseteq L_{N'}\big(o(1)\big),\ \alpha<1/2,$$

$o(1)$ 代表趋于零 (当 $N'\to\infty$ 时) 的实值函数的集合.

若能选取光滑性界 $\mathcal{S}$, 使得 $n'\in O\big(L_{N'}(\rho+o(1))\big)$ 和 $N/N_{\mathcal{S}}\in O\big(L_{N'}(\delta+o(1))\big)$, 其中 ρ 和 δ 是正常数. 由于 $N\in\widetilde{O}(N')$, 故 $L_N(c)\in O\big(L_{N'}(c)+o(1)\big)$, 而 N 可利用 2 次筛法在 $O\big(L_N(1+o(1))\big)\subseteq O\big(L_{N'}(1+o(1))\big)$ 的期望时间内分解. 再设 τ, 使得 $t_s\in\widetilde{O}(n'^{\tau})$, 于是 (16.9) 式就变为

$$O\big(L_{N'}(\max(1,2\rho,(1+\tau)\rho+\delta)+o(1))\big).$$

下面我们就是来考虑 $\mathcal{S}$ 的选取, 以使得上述关于 n' 和 $N/N_{\mathcal{S}}$ 的假定成立.

回顾 $N'=q^g$, 令 $\mathcal{S}=\lceil\log_q L_{q^g}(\rho)\rceil$, 易知 $n=\#\mathfrak{P}_{\mathcal{S}}\leqslant 2qL_{q^g}(\rho)$. 假定亏格 $g\geqslant\mathcal{V}\log q$, $\mathcal{V}$ 是某个正常数, 于是易知 $q\leqslant L_{q^g}(\frac{1}{\sqrt{\mathcal{V}}})$. 下面将证明

$$N_{\mathcal{S}}\geqslant q^g L_{q^g}\Big(-\frac{1}{2\rho}\Big),\tag{16.10}$$

从而 $N/N_S \in \widetilde{O}(N'/N_S) \subseteq O(L_{q^g}(\frac{1}{2\rho}+o(1)))$, 从而算法的运行时间为

$$O\left(L_{q^g}\left(\max\left\{2\rho+\frac{2}{\sqrt{\mathcal{V}}}, \rho+\frac{1}{2\rho}+\frac{1}{\sqrt{\mathcal{V}}}, 1\right\}+o(1)\right)\right).$$

上述表达式显然在 ρ 取

$$\min\left\{\frac{\sqrt{2}}{2}, \sqrt{\frac{1}{2}+\frac{1}{4\mathcal{V}}}-\frac{1}{2\sqrt{\mathcal{V}}}\right\}=\sqrt{\frac{1}{2}+\frac{1}{4\mathcal{V}}}-\sqrt{\frac{1}{4\mathcal{V}}}$$

时达到最小, 此时的整个运行时间为

$$O\left(L_{q^g}\left(\sqrt{2}\left(\sqrt{1+\frac{1}{2\mathcal{V}}}+\sqrt{\frac{1}{2\mathcal{V}}}\right)+o(1)\right)\right),$$

因此, 如果能够证明 (16.10) 式, 则我们就得到了如下结果:

定理 16.11 设 $\mathbb{F}_q$ 是一个 q 元有限域, $\mathcal{C}$ 为定义在 $\mathbb{F}_q$ 上的亏格为 g 的一条超椭圆曲线, 其 Jacobian 记为 $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_q)$, 假定 $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_q)$ 为循环群且其阶已知, 则当 $g/\log q$ 趋于无穷时, 存在一个亚指数概率型算法求解 $\mathrm{Jac}(\mathcal{C})(\mathbb{F}_q)$ 中的离散对数问题, 其所需期望时间为 $L_{q^g}(\sqrt{2}+o(1))$.

本节剩余的部分就是要证明不等式 (16.10). 设 $K=\mathbb{F}_q$ 是 q 元有限域,

$$H=Y^2+hY-f\in K[X,Y],$$

其中 $h\in K[X,Y]$, $f\in K[X]$, $\deg(f)=2g+1$ 不可约、无重因子, $\deg(h)\leqslant g$. H 的坐标环定义为 $K[H]:=K[X,Y]/(H)$, H 的函数域 $K(H)$ 定义为 $K[H]$ 的分式域, 它是 $K(X)$ 的一个 2 次扩张. $K[H]$ 是 $K[X]$ 在 $K(H)$ 中的代数闭包.

显然 $K[X]$ 的任一素理想 $\mathfrak{p}$ 正好就是由不可约多项式 p 生成的. 若 $\mathfrak{P}$ 是 $K[H]$ 中位于 $\mathfrak{p}$ 上的一个素理想, 则其次数定义为

$$\deg(\mathfrak{P})=\left[K[H]/\mathfrak{P}:K[X]/\mathfrak{p}\right]=\left[K[H]/\mathfrak{P}:\mathbb{F}_{q^{\deg(\mathfrak{p})}}\right].$$

由文献 [53] 知有下述 3 种情形:

(a) $Y^2+hY-f\equiv 0 \pmod p$ 在 $K[X]/\mathfrak{p}$ 中有两个解 b 和 $-b-v$, 则 $K[H]$ 中有两个素理想位于 $\mathfrak{p}$ 上, 它们是 $\mathfrak{P}=(p,b-Y)$ 和 $\overline{\mathfrak{P}}=(p,-b-v-Y)$, 从而 $\mathfrak{p}K[H]=\mathfrak{P}\overline{\mathfrak{P}}$, 它们的次数为 $\deg p$. 我们称 p, $\mathfrak{p}$, $\mathfrak{P}$ 和 $\overline{\mathfrak{P}}$ 是分裂的.

(b) 方程在 $K[X]/\mathfrak{p}$ 中有重根 b, 它对应于位于 $\mathfrak{p}$ 上的惟一的素理想 $\mathfrak{P}=(p,b-Y)$, 从而 $\mathfrak{p}K[H]=\mathfrak{P}^2$, $\mathfrak{P}$ 的次数是 $\deg p$, 而 p, $\mathfrak{p}$ 和 $\mathfrak{P}$ 称为分歧的.

(c) 方程在 $K[X]/\mathfrak{p}$ 中无解, 从而 $\mathfrak{P}=\mathfrak{p}K[H]$ 是 $K[H]$ 中位于 $\mathfrak{p}$ 上的惟一素理想, $\mathfrak{P}$ 的次数是 $2\deg p$, 而 $\mathfrak{p}$ 和 $\mathfrak{P}$ 称为惰性的.

现在设 $\mathfrak{U}$ 是 $K[H]$ 中一个理想, 则 $\mathfrak{U}$ 可以惟一分解为有限个素理想之积

$$\mathfrak{U} = \prod_i \mathfrak{P}_i^{e_i}.$$

$\mathfrak{U}$ 称为是本原的或半约化的, 如果 $\mathfrak{U}$ 没有主理想因子. 于是有下列性质:

(a) 每一个 $\mathfrak{P}_i$ 都不是惰性的 (因为惰性素理想是主理想);

(b) 若 $\mathfrak{P}_i$ 是分裂的, 则 $\overline{\mathfrak{P}}_i$ 不出现在分解式中 (因为 $\mathfrak{P}_i\overline{\mathfrak{P}}_i = (p_i)$ 是主理想);

(c) 若 $\mathfrak{P}_i$ 是分歧的, 则 $e_i = 1$(因为 $\mathfrak{P}_i^2 = (p_i)$ 是主理想).

素理想分解的惟一性表明这些条件是充分必要的.

定义 $\deg(\mathfrak{U}) = \sum_i e_i \deg \mathfrak{P}_i$. 一个半约化的理想称为是既约的, 如果它的次数 $\deg(\mathfrak{U})$ 不超过 g. 而任何一个半约化的理想可惟一地表示为以下形式:

$$\mathfrak{U} = (a, b - Y), \quad a, b \in K[X],\ \deg(b) < \deg(a)\text{ 且 }a|b^2 + hb - f.$$

$\mathfrak{U}$ 的素理想分解可如下决定: 写 $a = \prod_i p_i^{e_i}$, p_i 是不可约多项式, 则每一个 p_i 都不是惰性的 (因 b 是 $H \equiv O \bmod p_i$ 的一个解). 令 $b_i \equiv b \pmod{p_i}$, $\deg(b_i) < \deg(p_i)$ 且 $\mathfrak{P}_i = (p_i, b_i - Y)$, 则

$$\mathfrak{U} = \prod_i \mathfrak{P}_i^{e_i}.$$

更进一步, 有 $\deg(\mathfrak{U}) = \sum_i e_i \deg(\mathfrak{P}_i) = \sum_i e_i \deg(p_i) = \deg(a)$.

上面给出的理想论方法描述了超椭圆曲线

$$H:\ Y^2 + hY - f = 0$$

的仿射部分: $K[H]$ 的每一个素理想对应于 H 上的一个闭仿射点, 且诱导出 $K(H)$ 上一个赋值. 而由我们对 h 和 f 的假定, $K[X]$ 上的无穷赋值 (它由负次数给出) 是分歧的, 即曲线 C 有一个多重无穷远点.

不难看出, 在 H 的 Jacobian 簇的元素和约化的素理想之间存在着一个一一对应 [54]. 因此, 前面关于 Jacobian 簇的元素 (或既约除子) 能够借助既约理想来很好的叙述. 于是, 我们下面研究次数为 n 的、其素因子的次数不超过 m 的半约化理想的数目, 这样的理想称为是 m 光滑的, 而特别有趣的情形是 $n = g$, 它们是 m 光滑的既约理想的数目.

次数为 n 的 m 光滑的既约理想的计算可以看作如下的一个组合问题: 先考虑尺度不超过 m 的素理想的多少, 然后看它们能组合出多少个具有上面性质 (a)~(c) 的理想的数目.

设 $\pi_+(k)$, $\pi_0(k)$ 和 $\pi_-(k)$ 分别是次数为 k 的分裂、分歧和惰性不可约多项式的数目. 记 $\pi(k) = \pi_+(k) + \pi_0(k) + \pi_-(k)$, 令 $\pi_k(+) = \sum_{i=1}^{k} \pi_+(i)$. 每一个次数 k

的分裂或分歧素理想 $\mathfrak{P}=(p,b-Y)$ 都给出曲线 H 上的 k 个点, 其坐标位于 $\mathbb{F}_{q^k}$ 中, 但不在 $\mathbb{F}_{q^k}$ 的任何子域中. 具体而言, 若 $x_1,x_2,\cdots,x_k$ 是 p 在 $\mathbb{F}_{q^k}$ 中不同的根, 则这些点就是 $(x_1,b(x_1)),\cdots,(x_k,b(x_k))$. 若 $\mathfrak{P}=(p)$ 是次数 k 的惰性理想, 则 k 是偶数且 $\deg(p)=k/2$. 设 x 是 p 在 $\mathbb{F}_{q^{k/2}}$ 中的一个根, 因为 p 是惰性的, 方程 $Y^2+h(x)Y-f(x)=0$ 在 $\mathbb{F}_{q^{k/2}}$ 中无根, 但在 $\mathbb{F}_{q^k}$ 中有两个不相同的解 y 和 $\overline{y}$. 且 (x,y) 和 $(x,\overline{y})$ 是 C 上的两个点, 因此 $\mathfrak{P}$ 对应曲线上 k 个点, 这些点定义在 $\mathbb{F}_{q^k}$ 上, 但不定义在 $\mathbb{F}_{q^k}$ 的子域上.

我们约定 $\pi_-(i)=0(\forall i\in\mathbb{Z}/2\setminus\mathbb{Z}$, 即 i 为半整数时). 由于无穷远点是 $\mathbb{F}_q$ 有理点, 因此 C 的光滑射影模型上的 $\mathbb{F}_{q^k}$ 有理点的总数为

$$N_k=\sum_{i|k}\left(2i\pi_+(i)+i\pi_0(i)+i\pi_-\left(\frac{i}{2}\right)\right)+1, \tag{16.11}$$

由 Weil 定理, 有

定理 16.12

$$|N_k-q^k-1|\leqslant 2gq^{k/2}.$$

利用这个定理, 我们来证明下面的

定理 16.13 *次数不超过 k 的分裂不可约多项式的数目 $\pi_k(+)$ 满足*

$$\pi_k(+)\geqslant\frac{1}{2k}\big(q^k-2(g+1)(q^{k/2}+1)\big).$$

若 $0<\varepsilon\leqslant 1/4$ 且 $k\geqslant\frac{1}{\varepsilon}\log_q(2g+6+\sqrt{2})$, 则

$$\frac{1}{2k}(q^k-q^{k(\frac{1}{2}+\varepsilon)})\leqslant\pi_+(k)\leqslant\frac{1}{2k}(q^k+q^{k(\frac{1}{2}+\varepsilon)}).$$

证明 由 Weil 定理和 (16.11) 式, 有

$$q^k-2gq^{k/2}-\sum_{i=1}^{\infty}i\pi_0(i)-\sum_{i|k}i\pi_-\left(\frac{i}{2}\right)-1\leqslant\sum_{i|k}2i\pi_+(i)\leqslant q^k+2gq^{k/2}.$$

因为 $\sum_{i=1}^{\infty}i\pi_0(i)$ 是对所有分歧不可约多项式的次数求和, 且一个不可约多项式是分歧的当且仅当它整除 H 的判别式 h^2+f, 而 h^2+f 的次数不超过 $2(g+1)$, 故有 $\sum_{i=1}^{\infty}i\pi_0(i)\leqslant 2(g+1)$. 若 k 是奇数, 则 $\sum_{i|k}i\pi_-(\frac{i}{2})=0$, 否则, 它满足

$$\sum_{i|k/2}2i\pi_-(i)\leqslant 2\sum_{i|k/2}i\pi(i)=2q^{k/2},$$

从而

$$q^k-2(g+1)(q^{k/2}+1)\leqslant\sum_{i|k}2i\pi_+(i)\leqslant q^k+2gq^{k/2}, \tag{16.12}$$

由于 $\pi_k(+) = \sum_{i=1}^{k} \pi_+(i) \geqslant \frac{1}{2k}\sum_{i|k} 2i\pi_+(i)$, 定理 16.13 的第 1 个不等式由 (16.12) 式左边的不等号导出.

令 $g(k) = \sum_{i|k} 2i\pi_+(i)$, 则由 Möbius 反演公式给出 $2k\pi_+(k) = \sum_{i|k}\mu(k/i)g(i)$. 于是对 $k \geqslant \frac{1}{\varepsilon}\log_q\left(2g+6+\sqrt{2}\right)$, 利用 (16.12) 式有

$$
\begin{aligned}
2k\pi_+(k) &\geqslant g(k) - \sum_{i=1}^{\lfloor k/2 \rfloor} g(i) \\
&\geqslant q^k - (2g+2)q^{k/2} - (2g+3) - \sum_{i=1}^{\lfloor k/2 \rfloor}\left(q^i + 2gq^{i/2}\right) \\
&\geqslant q^k - (2g+2)q^{k/2} - \frac{q}{q-1}(q^{k/2}-1) - 2 - 2g\frac{\sqrt{q}}{\sqrt{q}-1}(q^{k/4}-1) - 2g - 1 \\
&\geqslant q^k - (2g+4)q^{k/2} - (2g+1)(2+\sqrt{2})q^{k/4} \\
&\geqslant q^k - (2g+4)q^{k/2} - (2+\sqrt{2})q^{k/2} \\
&\geqslant q^k - q^{k(\frac{1}{2}+\varepsilon)}.
\end{aligned}
$$

在上面得出倒数第 2 个不等式时, 用到了以下事实: $2g+1 \leqslant 2g+6\sqrt{2} \leqslant q^{k\varepsilon} \leqslant q^{k/4}$, 于是得出

$$
\pi_+(k) \geqslant \frac{1}{2k}\left(q^k - q^{k(\frac{1}{2}+\varepsilon)}\right).
$$

而 $\pi_+(k)$ 的上界也可类似推出, 定理证毕.

下面考察光滑半约化理想所占比例. 由定理 16.13 的证明过程, 知道分歧素理想的数目不超过 $2g+2$, 这是可忽略不计的. 现在我们将注意力集中到只有分裂素因子的理想上来. 定理 16.13 表明次数 k 的分裂素理想的数目是 $\frac{1}{k}(q^k + O(q^{\alpha k}))$, 其中 $\alpha < 1$.

令 $N(n,m)$ 是 $K[H]$ 中次数为 n 的 m 光滑半约化理想的数目.

定理 16.14　设 $m \geqslant \max\{8\log_q(2g+6+\sqrt{2}, 2\log_q((6+\frac{10}{3}\sqrt{2})n)\} + 2$, 且 $u = n/m$, 则

$$
N(n,m) \geqslant \frac{q^n}{2n^{\lceil u \rceil}}.
$$

证明　先假定 $m \leqslant n$. 由定理 16.13, 分裂素理想的数目随次数的增加而增长. 我们现在来计算一类特殊的半约化理想的数目, 这些半约化理想的素因子都具有相当高的次数. 为了保证一个理想的所有素因子均有较大的次数, 显然该理想应有尽可能多的素因子. 而对于一个 m 光滑的 n 次理想, 这意味着有 $\lceil u \rceil$ 个素因子. 我们尽可能均匀地分配这些素理想的次数. 令

$$
m_0 = \left\lfloor \frac{n}{\lceil u \rceil} \right\rfloor, \quad m_1 = m_0 + 1, \quad r_1 = n - \lceil u \rceil m_0, \quad r_0 = \lceil u \rceil - r_1.
$$

记 $\widetilde{N}(n,m)$ 是如下半约化理想的数目：这些半约化理想具有 r_0 个次数为 m_0 的不同的分裂素因子和 r_1 个次数为 m_1 的不同的分裂素因子. 由于 $n = m_0r_0 + m_1r_1$, 这些理想的次数为 n. 又由于 $m_0 \leqslant \frac{n}{\lceil u\rceil} \leqslant m$, 所以除非 $m_0 = m$ 且 $m_1 = m+1$, $r_1 > 0$, 则这些理想均是 m 光滑的. 但若 $m_0 = m$, $m_1 = m+1$, 则 $\lceil u\rceil$ 整除 n, 从而 $r_1 = 0$. 可见这样的理想一定是 m 光滑的, 从而 $N(n,m) \geqslant \widetilde{N}(n,m)$. 下面估计 $\widetilde{N}(n,m)$. 注意选取 r_i 个次数为 m_i 的分裂的不可约多项式的可能性有 $\binom{\pi_+(m_i)}{r_i}$ 种, 而每一个不可约多项式可以允许从两个素理想之一中选取 (因为分裂性), 因此

$$\begin{aligned}
\widetilde{N}(n,m) &= 2^{r_0}\binom{\pi_+(m_0)}{r_0}2^{r_1}\binom{\pi_+(m_1)}{r_1}\\
&\geqslant 2^{r_0+r_1}\frac{(\pi_+(m_0)-(r_0-1))^{r_0}(\pi_+(m_1)-(r_1-1))^{r_1}}{r_0!r_1!}\\
&\geqslant \frac{\sqrt{2}^{r_0+r_1-2}}{r_0^{r_0}r_1^{r_1}}2^{r_0+r_1}\frac{\left(q^{m_0}-q^{\frac{3}{4}m_0}-2m_0(r_0-1)\right)^{r_0}}{(2m_0)^{r_0}}\\
&\quad\times\frac{\left(q^{m_1}-q^{\frac{3}{4}m_1}-2m_1(r_1-1)\right)^{r_1}}{(2m_1)^{r_1}}\\
&\geqslant \frac{\sqrt{2}^{r_0+r_1-2}}{n^{\lceil u\rceil}}\left(q^{m_0}-q^{\frac{3}{4}m_0}-2n\right)^{r_0}\left(q^{m_1}-q^{\frac{3}{4}m_1}-2n\right)^{r_1}.
\end{aligned}$$

导出上述倒数第 2 个不等式时, 我们应用了事实 $r! \leqslant \frac{r^r}{\sqrt{2}^{r-1}}\ (\forall r \geqslant 0)$ 和定理 16.13 (取 $\varepsilon = \frac{1}{4}$, 注意 $m_1 > m_0 > \frac{n}{\frac{n}{m}-1} \geqslant \frac{1}{2}m-1$). 现在, $m_0 \geqslant 4\log_q(2g+6+\sqrt{2}) \geqslant 4\log_q(8+\sqrt{2})$, 从而 $q^{\frac{1}{4}m_0} \geqslant 8+\sqrt{2}$, $q^{\frac{3}{4}m_0} \leqslant q^{m_0}/(8+\sqrt{2})$, 类似地 $q^{\frac{3}{4}m_1} \leqslant q^{m_1}/(8+\sqrt{2})$. 又令 $c = 1-\frac{1}{8+\sqrt{2}}-\frac{1}{\sqrt{2}}$, 则由定理 16.14 对 m 的假设知, $2n \leqslant cq^{m_0} \leqslant cq^{m_1}$, 从而

$$\widetilde{N}(n,m) \geqslant \frac{\sqrt{2}^{r_0+r_1}}{2n^{\lceil u\rceil}}\cdot\frac{q^{m_0r_0}q^{m_1r_1}}{\sqrt{2}^{r_0}\sqrt{2}^{r_1}} = \frac{q^n}{2n^{\lceil u\rceil}}.$$

这就对 $m \leqslant n$ 证明了定理 16.14, 若 $m > n$, 则

$$N(n,m) = N(n,n) \geqslant \frac{q^n}{2n} = \frac{q^n}{2n^{\lceil u\rceil}}.$$

于是定理得证.

推论 16.1 条件如定理16.14中, 假设还有 $m \leqslant k\log n$(k 为一个正常数), 则

$$N(n,m) \geqslant \frac{q^n}{u^{u\left((1+\frac{1}{u})(1+\frac{\log(k\log n)}{\log u})+\frac{\log 2}{u\log u}\right)}} \in \frac{q^n}{u^{u(1+o(1))}},\quad u\to\infty.$$

证明　此时定理 16.14 中的不等式中的分母为

$$2n^{\lceil u\rceil}=2m^{\lceil u\rceil}u^{\lceil u\rceil}\leqslant 2(k\log n)^{u+1}=u^{u\left((1+\frac{1}{u})(1+\frac{\log(k\log n)}{\log u})+\frac{\log 2}{u\log u}\right)}.$$

而渐近结果是因为当 $u\to\infty$ 时, 有 $n\to\infty$, 从而

$$\frac{\log\log n}{\log u}\leqslant\frac{\log\log n}{\log n-\log(k\log n)}\to 0.$$

推论证毕.

定理 16.15　*设存在一个常数* $\varepsilon\in(0,1)$, *使得* m,n *和* $u=\frac{n}{m}$ *满足* $n^{1-\varepsilon}\geqslant m\geqslant\max\{16\log_q(2g+6+\sqrt{2})+4,\ 4\log_q((6+\frac{10}{3}\sqrt{2})n)+4,\log n\}$, $n\geqslant 2q$, $\frac{4}{\varepsilon}u\log u\geqslant 1$, *则*

$$N(n,m)\geqslant\frac{q^n}{u^{u\left(1+\frac{\log\log u+2+\log(4/\varepsilon)}{\log u}+\frac{3}{\varepsilon u}\right)}}\in\frac{q^n}{u^{(1+o(1))}},\ u\to\infty.$$

证明　在定理 16.14 的证明过程中, 我们计算了具有 $\lceil u\rceil$ 个次数为 m_0 或 m_0+1 的素因子的理想的个数, 从而得出了定理 16.14 中的不等式. 现在, 为了得出更多的光滑理想, 我们要放宽条件. 于是考虑具有 $\lfloor u\rfloor$ 个素因子的理想, 而每一个素因子的次数具有更大的变化范围.

更精确地说, 对于 $m\geqslant 5$ 和 $n\geqslant 2q$, 令

$$m-1\geqslant W:=\left\lfloor\left(1-\frac{1}{\log n}\right)m\right\rfloor\geqslant\left(1-\frac{1}{\log n}-\frac{1}{m}\right)m\geqslant\frac{m}{2}.$$

令 $\mathfrak{P}$ 是满足下述条件的素理想的集合：对于每一个分裂不可约多项式 p, $W+1\leqslant\deg(p)\leqslant m$, $\mathfrak{P}$ 中正好包含一个理想位于 p 上. 考虑形如 $U=U_1U_2$ 的理想, 其中 U_1 正好有 $\lfloor u\rfloor$ 个 $\mathfrak{P}$ 中的素因子 (不必相同), 而 U_2 是半约化的次数为 $n-\deg(U_1)$ 的 W 光滑理想. 由 $\mathfrak{P}$ 的构造知 U_1 是半约化的 m 光滑的理想, 且 U_1 和 U_2 无公共的素因子. 由于 $\deg(U)=n$, 因此这样的理想 U 的数目给出了 $N(n,m)$ 的一个下界. 记 $\mathfrak{J}$ 是所有可能的 U_1 的集合, 则上面的讨论表明

$$N(n,m)\geqslant\sum_{U_1\in\mathfrak{J}}N\big(n-\deg(U_1),W\big).$$

由于 $W\geqslant\frac{m}{2}$ 及加于 m 上的限制, 我们可以将定理 16.14 应用到目前的情形, 从而有

$$N(n-\deg(U_1),W)\geqslant\frac{q^{n-\deg(U_1)}}{2(n-\deg(U_1))^{\lceil\frac{n-\deg(U_1)}{W}\rceil}}.$$

上式右端分母的对数有以下上界：

$$\begin{aligned}\left(\frac{n-\deg(U_1)}{W}+2\right)\log n &\leqslant \left(\frac{n}{W}-(u-1)+2\right)\log n\\ &\leqslant \left(\left(\frac{1}{1-\frac{1}{\log n}-\frac{1}{m}}-1\right)u+3\right)\log n\\ &\leqslant \frac{2}{\log n-2}+3\log n \qquad (\text{因为} m\geqslant \log n)\\ &\leqslant 2u+\frac{3}{\varepsilon}\log u \qquad (\text{因为} \log n\geqslant 3 \text{且} n^{\varepsilon}\leqslant u),\end{aligned}$$

从而

$$N(n,m)\geqslant \frac{q^n}{u^{u\left(\frac{2}{\log u}+\frac{3}{\varepsilon u}\right)}}\sum_{U_1\in\mathfrak{J}} q^{-\deg(U_1)} \tag{16.13}$$

上式右边的和式可如下计算：令 $\mathfrak{P}=\{\mathfrak{P}_1,\mathfrak{P}_2,\cdots,\mathfrak{P}_l\}$, 则由二项式定理有

$$\begin{aligned}\sum_{U_1\in\mathfrak{J}} q^{-\deg(U_1)} &= \sum_{a_i\geqslant 0, a_1+\cdots+a_l=\lfloor u\rfloor} q^{-a_1\deg(\mathfrak{P}_1)-\cdots-a_l\deg(\mathfrak{P}_l)}\\ &\geqslant \frac{\left(\sum_{i=1}^{l} q^{-\deg(\mathfrak{P}_i)}\right)^{\lfloor u\rfloor}}{\lfloor u\rfloor!}\\ &\geqslant u^{-\lfloor u\rfloor}\left(\sum_{j=W+1}^{m}\pi_+(j)q^{-j}\right)^{\lfloor u\rfloor} \qquad (\text{因} \deg(\mathfrak{P}_i)\geqslant W+1)\\ &\geqslant u^{-\lfloor u\rfloor}\left(\sum_{j=W+1}^{m}\frac{1}{2j}\left(1+\frac{1}{q^{j(\frac{1}{2}-\frac{1}{8})}}\right)\right)^{\lfloor u\rfloor} (\text{定理 } 16.13, \varepsilon=\frac{1}{8})\\ &\geqslant u^{-\lfloor u\rfloor}\left(\frac{1}{4}\sum_{j=W+1}^{m}\frac{1}{j}\right)^{\lfloor u\rfloor} \qquad (\text{因} q^{\frac{3}{8}(W+1)}\geqslant 2^{\frac{3}{2}}>2)\\ &\geqslant u^{-\lfloor u\rfloor}\left(\frac{m-W}{4m}\right)^{\lfloor u\rfloor}\geqslant (4u\log n)^{-\lfloor u\rfloor}\\ &\geqslant \left(\frac{4}{\varepsilon}u\log u\right)^{-\lfloor u\rfloor}\geqslant \left(u^{1+\frac{\log\log u+\log\frac{4}{\varepsilon}}{\log u}}\right)^{-\lfloor u\rfloor}.\end{aligned} \tag{16.14}$$

由 (16.13) 和 (16.14) 式就得到定理的结果.

考虑光滑理想的数目. 为简化记号, 令

$$L(\rho)=e^{\rho\sqrt{(g\log q)\log(g\log q)}}$$

为输入尺度为 $g\log q$ 的亚指数函数. 因为我们要考虑的是既约理想, 故令 $n=g$, 在次数不超过 m 的因子基中, 共有 $O(q^m)$ 个素理想. 令

$$m=\lceil \log_q L(\rho)\rceil=\left\lceil \rho\sqrt{\frac{g\log(g\log q)}{\log q}}\right\rceil,$$

此处 $\rho > 0$ 是一个 (待定) 常数. 我们的目的是利用推论 16.1 和定理 16.15 获得 $g \to \infty$ 时的渐近结果. 注意推论 16.1 和定理 16.15 的条件对任意 $\varepsilon \in (0, \frac{1}{2})$ 和充分大的 g 均满足. 因为当 $g \to \infty$ 时, 有 $u \to \infty$, 故有

$$N(g,m) \geqslant \frac{q^g}{u^{u(1+\alpha(g))}}, \quad \lim_{g\to\infty} \alpha(g) = 0. \tag{16.15}$$

在此情形下有

$$u = \frac{g}{m} \leqslant \frac{1}{\rho}\sqrt{\frac{g\log q}{\log(g\log q)}} \leqslant \frac{1}{\rho}\sqrt{g\log q},$$

从而

$$\log u \leqslant \frac{1}{2}\log(g\log q) - \log\rho,$$

而不等式 (16.15) 的右端的分母之对数满足

$$\begin{aligned}(1+\alpha(g))u\log u &\leqslant \frac{1}{2\rho}(1+\alpha(g))\Big(1 - \frac{2\log\rho}{\log(g\log q)}\Big)\sqrt{(g\log q)\log(g\log q)}\\ &\in \Big(\frac{1}{2\rho} + o(1)\Big)\sqrt{(g\log q)\log(g\log q)}.\end{aligned}$$

从而我们证明了下述结果:

定理 16.16　*设 $\rho > 0$ 为常数, $m = \lceil \log_q L(\rho) \rceil$, 则存在一个函数 $\beta(g) \in o(1)$(当 $g \to \infty$ 时), 使得*

$$N(g,m) \geqslant L\Big(-\frac{1}{2\rho} - \beta(g)\Big)q^g.$$

这就是我们需要的不等式 (16.10), 从而定理 16.11 得到了完整的证明.

注记: 离散对数的指标计算法是目前计算各种离散对数的最有效的方法. 本章的主要内容的写作参考了以下文献: Gaudry, An algorithm for solving discrete log problem on hyperelliptic curves, In B. Preneel, editor, Advances in Crypyology-Eurocrypt 2000, Volume 1807 of Lecture Notes in Computer Science, Pages 19–34, Springer-Verlag, 2000.

第十七章　椭圆曲线离散对数的代数几何攻击方法

§17.1　Weil 下降与 Weil 攻击

设 H/K 是定义在一个有限非素数域 K 上的椭圆曲线或超椭圆曲线, 假设除子类群 $CL^\circ(H/K) = \mathrm{Jac}(H)(K)$($H/K$ 上次数为 0 的除子类群) 上的离散对数问题 (Discrete Logarithm Problem, 以后简记为 DLP) 用于密码目的. 注意当 E 是椭圆曲线时, 我们有一个典范同构 $E(K) \cong CL^\circ(E/K)$, 从而可以考虑椭圆曲线上的 DLP 问题.

假定 DLP 问题用于密码学目的, 特别地意味着 $CL^\circ(H/K)$ 包含一个大素数阶的子群, 下面就要用到这个事实.

若 H 的亏格不小于 4, 则前面介绍的 $CL^\circ(H/K)$ 上的指标计算攻击方法比一般的攻击方法如 Pollard ρ 方法等更为有效, 因此其安全性比较低. 因而我们的基本想法是将 $CL^\circ(H/K)$ 中的 DLP 问题转化为某个更小的域上亏格更高的曲线的类群中的 DLP 问题. 而后者可以有较有效的攻击方法, 如指标计算攻击方法.

现在假设 K 是另一个有限域 k 的一个扩张, 域 k 不必是一个素域. 我们固定以下记号: $p = \mathrm{char}(k)$, $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$, 即 $[K:k] = n$. 设有一个清晰给定的定义在 k 上的曲线 $\mathcal{C}/k$, 以及一个清晰给定的定义在 K 上的覆盖 $C: \mathcal{C} \to H$ (称两条曲线之间的一个非常数态射为一个覆盖).

于是有所谓余范映射或拉回映射

$$C^*:\ Cl^\circ(H/K) \to Cl^\circ(\mathcal{C}/K),$$

同时, 也有所谓范映射 $N:\ Cl^\circ(\mathcal{C}/K) \to Cl^\circ(\mathcal{C}/k)$. 复合这两个映射, 则获得以下的映射:

$$N \circ C^*:\ Cl^\circ(H/K) \to Cl^\circ(\mathcal{C}/k). \tag{17.1}$$

更进一步, 假设 $Cl^\circ(H/K)$ 中的大素数阶子群在此映射下保持不变, 即设它不在映射 (17.1) 的核中, 则可以试着将 $Cl^\circ(H/K)$ 中的 DLP 问题映射到 $Cl^\circ(\mathcal{C}/k)$ 中, 从而利用指标计算攻击法在后面的群中来解决该 DLP 问题. 以后称 H/K 中 DLP 问题的此类攻击为几何覆盖攻击, 简称为几何攻击.

如果群 $Cl^\circ(H/K)$ 的阶是几乎素数 (即为一个小正整数乘上一个大素数的形式), 则 $\mathcal{C}$ 的亏格将至少等于 $g(H)n$, 此处 $g(H)$ 是 H 的亏格. 下面说明这一点: 由假设群 $Cl^\circ(H/K)$ 的阶为几乎素数及假设映射 (17.1) 的核不含大素数阶子群, 知

$N \circ C^*$ 的核非常小, 设它是平凡的. 于是 $N \circ C^*$ 为单射, 从而 $\log_q(\#Cl^\circ(\mathcal{C}/k)) \geqslant \log_q(\#Cl^\circ(H/K))$. 再由 Hasse-Weil 界, 知

$$\log_q(\#Cl^\circ(\mathcal{C}/k)) \sim g(\mathcal{C}), \quad \log_q(\#Cl^\circ(H/K)) \sim g(H)n,$$

因此得到

$$g(\mathcal{C}) \geqslant g(H)n. \tag{17.2}$$

有时候在密码学应用中, 我们需要考虑下述应用：设曲线 H 定义在 k 上, 但在 K 上考虑它, 则 $Cl^\circ(H/K)$ 包含 $Cl^\circ(H/k)$. 另一方面, $Cl^\circ(H/K)$ 包含另一个群 $\mathrm{Ker}(N)$, 称之为迹零群 (trace-zero group), 在绝大多数应用中, 迹零群与 $Cl^\circ(H/k)$ 在 $Cl^\circ(H/K)$ 中的交为平凡的. 若假定迹零群的阶是几乎素数, 则可以在密码学中应用这个迹零群中的 DLP 问题.

与前类似, 为了保证能将这个 DLP 问题化归到 $Cl^\circ(\mathcal{C}/k)$ 中的 DLP 问题, 我们假定迹零群的大素因子部分在上述映射下保持不变. 在此条件下, 可以用类似前面的推理给出

$$g(\mathcal{C}) \geqslant g(H)(n-1). \tag{17.3}$$

从实用角度而言, 不等式 (17.3) 与 (17.2) 只有在 n 较小时才有差别.

注意到 $Cl^\circ(\mathcal{C}/k)$ 中 DLP 问题的各种攻击方法将随着 $g(\mathcal{C})$ 的增长而失效, 因此, 在实际攻击中具有重要意义的是 $g(\mathcal{C})$ 要尽可能地小.

现在总结一下需要做的工作：我们需要一个清晰给定的曲线 $\mathcal{C}/k$ 及一个定义在 K 上的从 $\mathcal{C}$ 到 H 的态射 C, 使得

(a) $N \circ C^*$ 的核不包含 $Cl^\circ(H/K)$ 中的素数阶大子群;

(b) $\mathcal{C}$ 的亏格 $g(\mathcal{C})$ 不能太大.

更进一步, 最好是曲线 $\mathcal{C}$ 是超椭圆的或者是由另一类容易的方程所给出 (例如是 superelliptic), 而且 $\mathcal{C}$ 的同构还可以更进一步加快速度.

为了达到上述目的, 需要引进 Weil 限制和 Weil 下降的概念.

设 K/k 是有限域的一个次数为 n 的扩张, V 是定义在 K 上的一个仿射 (或射影) 簇, 则存在一个 n 维仿射 (或射影) 簇 W/k 以及一个定义在 K 上的态射 $u: W \to V$, u 具有以下的泛性质：

对每一个定义在 k 上的簇 X 及每一个定义在 K 上的态射 c: $X \to V$, 存在惟一的定义在 k 上的态射 a: $X \to W$, 使得 $c = u \circ a$, 即图 17.1 是交换的：

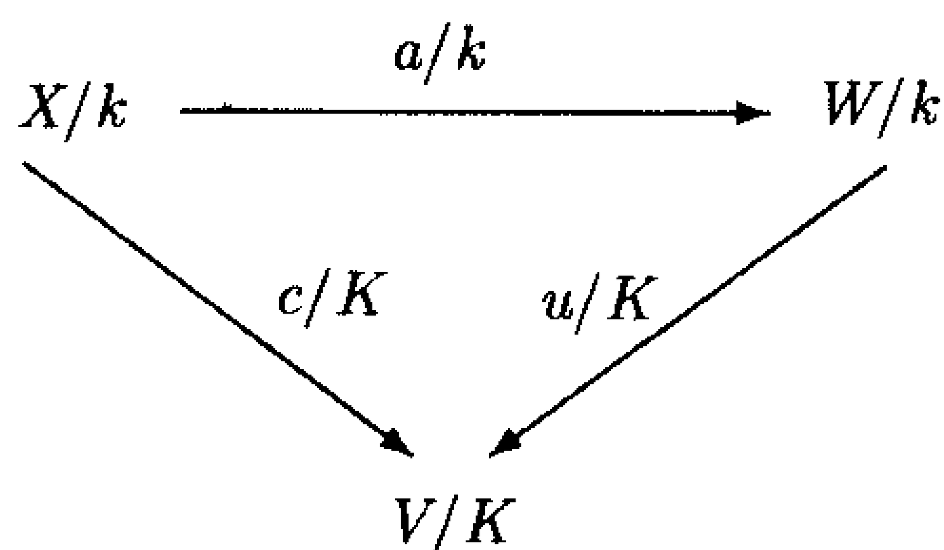


图 17.1

特别地, 这意味着在 $\mathrm{Mor}_K(X,V)$ 和 $\mathrm{Mor}_k(X,W)$ 间存在一个一一对应. 此处 $\mathrm{Mor}_K(X,V)$ 表示定义在 K 上的从 X 到 V 的态射的集合, 而 $\mathrm{Mor}_k(X,W)$ 表示定义在 k 上的从 X 到 W 上的态射的集合.

上面的簇 W/k 在同构意义下是惟一的, 它称为 V 关于 K/k 的 Weil 限制, 而这个过程称为 Weil 下降. 关于 Weil 限制的详细情形, 请参阅文献 [55].

我们将 Weil 限制的泛性质应用到簇 X 正好是一个点的情形. 令 X 是一个点, 则从 X 到 V 的定义于 K 上的态射正好是 V 中坐标全部位于 K 中的点, 这样的点称为 K 有理点, 全体 K 有理点的集合记为 $V(K)$. 于是十分清楚地, 若给定一个从点 X 到 V 的态射, 则得到一个 V 中的 K 有理点, 它就是 X 在该态射下的像. 反之, 若给定 V 上一个 K 有理点 P, 则得到从 X 到 V 的一个态射 $X \to V$, 它映射 X 到 P.

上述考虑可以对定义在 k 上从 X 到 W 的态射和 W 的 k 有理点进行, 因此, 有下述典范双射:

$$V(K) \cong \mathrm{Mor}_K(X,V), \quad W(k) \cong \mathrm{Mor}_k(X,W),$$

结合上面的双射 $\mathrm{Mor}_k(X,W) \cong \mathrm{Mor}_K(X,V)$, 我们看到

$$V(K) \cong W(k). \tag{17.4}$$

有时候, 在一个簇上可以定义一个代数群律: V 上的一个代数群律是一个态射 $m\colon V \times V \to V$, 使得对所有域扩张 λ/k, $V(\lambda)$ 在运算 $P+Q=m(P,Q)$ 的意义下是一个群. 定义在 K 上的一个簇如果具有一个定义在 K 上的代数群律, 就称为 K 上的群簇. 射影群簇称为 Abel 簇 (abelian varieties). 可以证明一个 Abel 簇上的群律一定是交换的, 而 1 维的 Abel 簇就是椭圆曲线.

若 V 是一个群簇, 则在 V 的 Weil 限制 W 上存在定义在 k 上的典范代数群律. 于是 W 成为 k 上的一个群簇. 现在集合 $V(K)$ 和 $W(k)$ 都是群, 且 (17.4) 式事实上是一个群同构, 特别地, 若 E 是定义在 K 上的一条椭圆曲线, 而 W/k 是 E 关于 K/k 的 Weil 限制, 则得到一个同构

$$E(K) \cong W(k). \tag{17.5}$$

而 Weil 限制在几何攻击中的重要性可以由下述泛性质得出:

定理 17.1 *若 H/K 是一条超椭圆曲线, 而 C/k 是另一条曲线, 且有一个态射 $c\colon C \to H$, 该态射定义在 K 上, 则有惟一一个定义在 k 上的态射 $a\colon C \to W$, 此处 W 是 H 关于 K/k 的 Weil 限制. 反之亦然.*

若有这样一个态射：$a: C \to W$, 便可以研究它在 W 中的像. 在此意义下, 寻找 W/k 上的曲线就等同于寻找曲线 C/k 及定义在 K 上的态射 $C \to H$. 从而, 在 W/k 上寻找曲线就是一种使覆盖攻击的一般想法清晰化的可能途径.

下面给出构造 Weil 限制的方法：设 V 是一个仿射簇, 选取 V 在 K 上的坐标函数 $X_1, \cdots, X_n$, 以及 K/k 的一组基 $(u_1, \cdots, u_m)$. 定义 $m \cdot n$ 个变量 $Y_{i,j}$ 如下：

$$X_i = u_1 Y_{1,i} + \cdots + u_m Y_{m,i}.$$

将此带入定义 V 的方程关系之中, 并将结果的关系的系数表为基 $(u_1, \cdots, u_m)$ 的线性组合, 然后比较这组基的系数以获得 W/k 的坐标函数 $Y_{1,1}, \cdots, Y_{m,n}$ 的定义关系式.

若 V 是拟射影簇, 则需要选取 V 的一个仿射覆盖, 对每一个仿射子簇, 应用上述 Weil 下降过程, 然后利用代数几何中的黏合技巧, 将这些获得的 k 上的仿射簇黏合成我们所需要的 W 即可.

例 17.1 设 $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$, $\mathrm{Char}(k) = 2$, $\{\psi_0, \cdots, \psi_{n-1}\}$ 是 K/k 的一组基. 设

$$E/K:\ Y^2 + XY = X^3 + \beta, \quad \beta \in K \tag{17.6}$$

是 K 上的一条椭圆曲线. 我们来寻找 E/K 的 Weil 限制 W/k. 令

$$\begin{aligned} \beta &= b_0\psi_0 + b_1\psi_1 + \cdots + b_{n-1}\psi_{n-1}, \\ X &= x_0\psi_0 + x_1\psi_1 + \cdots + x_{n-1}\psi_{n-1}, \\ Y &= y_0\psi_0 + y_1\psi_1 + \cdots + y_{n-1}\psi_{n-1}, \end{aligned} \tag{17.7}$$

其中 $b_i \in k$ 为常量, $x_i, y_i \in k$ 为变量. 将上述表达式带入 (17.6) 式, 有

$$\begin{aligned} &(y_0\psi_0 + y_1\psi_1 + \cdots + y_{n-1}\psi_{n-1})^2 + (x_0\psi_0 + x_1\psi_1 + \cdots + x_{n-1}\psi_1) \\ &\times (y_0\psi_0 + y_1\psi_1 + \cdots + y_{n-1}\psi_{n-1}) \\ = &(x_0\psi_0 + x_1\psi_1 + \cdots + x_{n-1}\psi_{n-1})^3 + b_0\psi_0 + b_1\psi_1 + \cdots + b_{n-1}\psi_{n-1}. \end{aligned}$$

将上式各项展开后, 将等式表示成 $\psi_0, \psi_1, \cdots, \psi_{n-1}$ 的线性组合, 然后比较 ψ_i 前的关系式, 就得出了定义 A/k 的方程组. 它是定义在 k 上的一个 n 维 Abel 簇. 这就是 E/K 关于 K/k 的 Weil 限制.

下面考虑一种特殊情形：假定域 K 中存在一组形如 $\psi_i = \theta^{2^i}$ 的基, 使得 $\theta + \theta^2 + \theta^4 + \cdots + \theta^{2^{n-1}} = 1$. 为了产生 A 中低亏格的曲线, 应当寻找低次数的曲线. 这可以通过超平面 $x_0 = x_1 = \cdots = x_{n-1} = x$ 与 A 相交得到. 因此, 考虑将 X 限制在

k 中而得到的 A 的子簇, 于是得到一条由下述方程定义的曲线:

$$\mathscr{C}: \quad \begin{cases} y_{n-1}^2 + xy_0 + x^3 + b_0 = 0, \\ y_0^2 + xy_1 + x^3 + b_1 = 0, \\ \qquad \vdots \\ y_{n-2}^2 + xy_{n-1} + x^3 + b_{n-1} = 0. \end{cases}$$

之所以能得到如此的稀疏方程式, 是由于假定了 K/k 有上述形式的基. 消去变量, 就产生了一条关于 x 和 $y(=y_0)$ 的曲线

$$\mathscr{C}: \quad y^{2^n} + x^{2^n-1}y + \sum_{i=0}^{n-1} x^{2^n+2^i} + g(x) = 0,$$

其中 $g(x)$ 是一个次数不大于 2^n 的多项式, 它与 $b_0, \cdots, b_{n-1}$ 有关:

$$g(x) = \sum_{i=1}^{n} b_i^{2^{n-i}} x^{2^n-2^{n-i+1}},$$

其中 $b_n = b_0$.

例 17.2 接着例 17.1, 考虑 $n = 2, 3, 4$ 的情形.

(1) $n = 2$, 则

$$\mathscr{C}_2: \quad y^4 + x^3y + x^6 + x^5 + b_0x^2 + b_1^2 = 0.$$

若原先的椭圆曲线定义在基域上, 即 $b_0 = b_1$, 则 $\mathscr{C}_2$ 有两个不可约分支, 每一个都是一条椭圆曲线, 否则, 它是不可约的. 此时, 将参数 b_0 和 b_1 用 k 中元素代入后, 该曲线的亏格看起来总是 2.

(2) $n = 3$, 则

$$\mathscr{C}_3: \quad y^8 + x^7y + x^{12} + x^{10} + x^9 + b_0x^6 + b_2^2x^4 + b_1^4 = 0.$$

曲线 $\mathscr{C}_3$ 在 $b_0 = b_1 = b_2$ 时可约 (此时原先的椭圆曲线定义在 k 上), 否则 $\mathscr{C}_3$ 不可约. 经过计算, 该曲线的亏格似乎总是 3 或 4.

(3) $n = 4$, 则

$$\mathscr{C}_4: y^{16} + x^{15}y + x^{24} + x^{20} + x^{18} + x^{17} + b_0x^{14} + b_3^2x^{12} + b_2^4x^8 + b_1^8 = 0.$$

实际计算, 当该曲线不可约时, 其亏格似乎总不超过 8, 当 $b_3 = b_0 + b_1 + b_2$ 时, 该曲线可约, 其中一个分支由下式给出:

$$\mathscr{C}_{4a}: y^8 + x^4y^4 + x^6y^2 + x^7y + x^{12} + x^9 + b_0x^6 + (b_2^2 + b_1^2)x^4 + b_1^4 = 0.$$

当 $\mathscr{C}_{4a}$ 不可约时, 计算经验表明其亏格似乎不超过 4.

§17.2 特征 2 的 GHS 攻击

设 K/k 是特征 2 的 n 次扩张, k 的元素个数为 q. 而

$$E/K: Y^2+XY=X^3+\alpha X^2+\beta, \quad \alpha,\beta\in K,\ \beta\neq 0.$$

我们可以如上节例 17.1 中构造 E/K 关于 K/k 的 Weil 限制 A/k, 为简单起见, 假定 K/k 的基元素之和为 1. 将结果的 Abel 簇 A 与超平面相交, 就给出 A 的一个子簇. 它实际上是 $n+1$ 维空间中一条定义在 k 上的曲线. 与上节例 17.1 中类似, 将其记为 $\mathscr{C}$. 下面从几何角度研究该曲线 $\mathscr{C}$. 于是将 $\mathscr{C}$ 视为 k 的代数闭包中的曲线.

引理 17.1 通过定义在 K 上的变量的线性变换 $y_i\to w_i$, 发现 $\mathscr{C}$ 双有理等价于下述定义在 K 上的曲线:

$$\mathfrak{D}:\quad \begin{cases} w_0^2+xw_0+x^3+\alpha_0x^2+\beta_0=0,\\ \qquad\vdots\\ w_{n-1}^2+xw_{n-1}+x^3+\alpha_{n-1}x^2+\beta_{n-1}=0,\end{cases}$$

其中 $\alpha_j=\sigma^j(\alpha)$, $\beta_j=\sigma^j(\beta)$, σ 是 K/k 上的Frobenius自同构.

我们可以扩充Frobenius自同构 σ 到 $K[x,w_0,\cdots,w_{n-1}]$: $\sigma(x)=x$, $\sigma(w_i)=w_{i+1}$, $0\leqslant i<n-1$, $\sigma(w_{n-1})=w_0$, 则有 $\sigma(y_i)=y_i$, $0\leqslant i\leqslant n-1$.

证明 首先证明关于 Frobenius 自同构的叙述. σ 显然可以如所述扩充到 $K[x,w_0,\cdots,w_{n-1}]$. 令

$$T=\left(\sigma^j(\psi_i)\right)_{0\leqslant i,j\leqslant n-1}\in K^{n\times n},$$

则 T 是可逆的. 于是引理中的变量线性变换为 $(w_0,\cdots,w_{n-1})=(y_0,\cdots,y_{n-1})T$. 令 t_i 记 T 的第 i 列, y_i 可表为 w_i 的 K 线性组合

$$(y_0,\cdots,y_{n-1})=(w_0,\cdots,w_{n-1})T^{-1}.$$

将 σ 应用到 $(w_0,\cdots,w_{n-1})=(y_0,\cdots,y_{n-1})T$, 有

$$(w_1,\cdots,w_{n-1},w_0)=\left(\sigma(y_0),\cdots,\sigma(y_{n-1})\right)(t_1,\cdots,t_{n-1},t_0).$$

另一方面, 由 $(w_0,\cdots,w_{n-1})=(y_0,\cdots,y_{n-1})T$, 直接可知

$$(w_1,\cdots,w_{n-1},w_0)=(y_0,\cdots,y_{n-1})(t_1,\cdots,t_{n-1},t_0),$$

从而

$$(\sigma(y_0),\cdots,\sigma(y_{n-1}))(t_1,\cdots,t_{n-1},t_0)=(y_0,\cdots,y_{n-1})(t_1,\cdots,t_{n-1},t_0).$$

由矩阵 $(t_1,\cdots,t_{n-1},t_0)$ 的可逆性, 有 $\sigma(y_i)=y_i$.

下面证明$\mathscr{C}$和$\mathfrak{D}$的双有理等价性. 设$\psi_0,\cdots,\psi_{n-1}$是K/k 的一组基, 且 $\sum\psi_i=1$. $\mathscr{C}$ 的方程可通过在 E 中代入

$$Y=\sum y_i\psi_i,\quad \alpha=\sum a_i\psi_i,\quad \beta=\sum b_i\psi_i,\quad X=x,$$

并比较 ψ_i 的系数而得到. 我们获得 $f_i\in k[x,y_0,\cdots,y_{n-1}]$, 使得

$$w_0^2+xw_0+x^3+\alpha_0x^2+\beta_0=\sum_{i=0}^{n-1}f_i(x,y_0,\cdots,y_{n-1})\psi_i.$$

而定义曲线 $\mathscr{C}$ 的方程是:

$$\mathscr{C}:\quad\begin{cases}f_0(x,y_0,\cdots,y_{n-1})=0,\\ \qquad\vdots\\ f_{n-1}(x,y_0,\cdots,y_{n-1})=0.\end{cases}$$

令 $g_i\in K[x,w_0,\cdots,w_{n-1}]$ 记 $\mathfrak{D}$ 的左端第 i 个多项式. 将 T 作用到 $(f_i(x,y_0,\cdots,y_{n-1}))_{0\leqslant i\leqslant n-1}$ 上, 有

$$\begin{aligned}(f_i(x,y_0,\cdots,y_{n-1}))_{0\leqslant i\leqslant n-1}\cdot T&=\Big(\sum_i f_i(x,y_0,\cdots,y_{n-1})\sigma^j(\psi_i)\Big)_{0\leqslant j\leqslant n-1}\\&=\Big(\sigma^j\Big(\sum_i f_i(x,y_0,\cdots,y_{n-1})\psi_i\Big)\Big)_{0\leqslant j\leqslant n-1}\\&=(\sigma^j(w_0^2+xw_0+x^3+\alpha_0x^2+\beta_0))_{0\leqslant j\leqslant n-1}\\&=(g_i(x,w_0,\cdots,w_{n-1}))_{0\leqslant i\leqslant n-1}.\end{aligned}$$

这表明 $\mathscr{C}$ 被 T 线性地变换到 $\mathfrak{D}$ 里, 从而 $\mathscr{C}$ 和 $\mathfrak{D}$ 是双有理等价的, 证毕.

现在令 F_i 是定义曲线 $\mathfrak{D}$ 的第 i 个方程在 $K(x)$ 上的分裂域. 则有

引理 17.2 我们能够在 $K(x)$ 上形成合成域 $F=F_0F_1\cdots F_{n-1}$. 设 $m\in\mathbb{Z}$, 使得 $[F:K(x)]=2^m$, 则作为 K 上的曲线 $\mathfrak{D}$ 具有 2^{n-m} 个不可约既约分支, 每一个分支的函数域都 K- 同构于 F.

证明 因为每一个扩张 $F_i/K(x)$ 是 2 次的, 从而是 Galois 扩张, 因此, 可以无歧义地形成合成域 F (the compositum without ambiguity). 更特别地, 为了在 $K(x)$ 上生成 F, 我们选取了方程组 $\mathfrak{D}$ 中适当的 m 个方程所组成的子集合, 使得在 $K(x)$

上邻接上 $w_{l_i}(0 \leqslant i \leqslant m)$ 后, 得出 F, 其中 w_i 是第 i 个这种方程的左端的一个根. $\mathfrak{D}$ 的剩下的 $n-m$ 个方程中每一个在 F 中具有 2 个根 $\overline{w}_{v_j}$ 和 $\overline{w}_{v_j}+x$(我们用到了 K 的特征为 2 这个事实).

考虑同态映射

$$\phi:\ K[x,w_0,\cdots,w_{n-1}] \longrightarrow K[x,\overline{w}_0,\cdots,\overline{w}_{n-1}] \subseteq F,$$

这个同态的核 I 是维数为 1 的素理想 (这是因为 F 是 K 上一个超越次数为 1 的域, 且 F 在 K 上由 $x,\overline{w}_0,\cdots,\overline{w}_{n-1}$ 生成). 由 F 的构造, I 包含 $\mathfrak{D}$ 的左端的多项式集, 因此, I 定义了 $\mathfrak{D}$ 的一个不可约既约分支, 其函数域 K 同构于 F.

而引理中关于这些不可约分支的数目的叙述是由于上述同态 ϕ 的定义中可能的 $\overline{w}_{v_j}$ 或 $\overline{w}_{v_j}+x$ 的选取. 事实上, 假设 I 包含在一个如上同态 ψ 的核 J 中 (ψ 将 $\overline{w}_{v_j}$ 映到 $\overline{w}_{v_j}+x$), 则存在 $f,g \in k[x,w_0,\cdots,w_{m-1}]$, 使得 $\phi(g)$, $\psi(g) \neq 0$ 且 $\overline{w}_{v_j} = \phi(f)/\phi(g) = \psi(f)/\psi(g)$. 于是 $gw_{v_j}+f \in I \subseteq J$ 且 $g(w_{v_j}+x)+f \in J$, 从而 $gx \in J$, 因此 $x \in J$(因 $\psi(g) \neq 0$, 而 J 是素理想), 从而 $\psi(x)=0$. 这是一个矛盾, 因为 x 不可能被 ψ 映到零. 这就证明了在选取 $\overline{w}_{v_j}$ 和 $\overline{w}_{v_j}+x$ 时, 对应互不包含的素理想, 从而对应互不相同的不可约既约分支. 对应于 $n-m$ 个方程的每一个都有两种选择, 而每一种选择对应一个不可约既约分支, 从而共有 2^{n-m} 个不可约既约分支, 证毕.

为了进一步研究曲线 $\mathfrak{D}$ 的性质, 我们将 $\mathfrak{D}$ 的方程两端同时乘上 x^{-2}, 并做变量替换 $s_i = w_i/x + \beta_i^{1/2}$, $z=1/x$, 则得到

$$\mathscr{F}:\ \begin{cases} s_0^2+s_0+z^{-1}+\alpha_0+\beta_0^{1/2}z=0, \\ \qquad\vdots \\ s_{n-1}^2+s_{n-1}+z^{-1}+\alpha_{n-1}+\beta_{n-1}^{1/2}z=0. \end{cases}$$

下面利用 Atrin-Schreier 理论研究上面的曲线 $\mathscr{F}$. 首先需要下述 Artin-Schreier 理论的主要结果:

定理 17.2 设 p 为一个素数, $\wp(x)=x^p-x$ 是Artin-Schreier算子. 设 K 是一个特征 p 的域, 固定 K 的一个可分闭包 $\overline{K}$, 记 K^+ 为 K 的加群. 对每一个加法子群 $\Delta \leqslant K^+$(使得 $\wp(K) \subseteq \Delta \subseteq K$) , 存在一个域 $L=K(\wp^{-1}(\Delta))$(即 L 是将所有多项式 x^p-x-d, $d\in\Delta$, 在 $\overline{K}$ 中的所有根加到 K 上得出的域), 显然有 $K\subseteq L\subseteq\overline{K}$. 于是有映射

$$\pi:\quad \Delta \longmapsto L=K(\wp^{-1}(\Delta)),$$

则 π 定义了一个从上述 K^+ 的加法子群 Δ 到 $\overline{K}$ 中指数为 p 的 Abel 扩张 L/K 之间的一一对应.

证明参见文献 [56].

引理 17.3 设 m 如引理17.2中所述, 则有

$$m = \dim_{\mathbb{F}_2}(\mathrm{Span}_{\mathbb{F}_2}\{(1, \beta_0^{1/2}), \cdots, (1, \beta_{n-1}^{1/2})\}). \tag{17.8}$$

而域 K 正好是 F 的常数域 (即 K 在 F 中是代数闭的), 且 F 是前 m 个域 F_i 在 $K(z)$ 上的合成域, 即 $F = F_0 \cdots F_{m-1}$(在 $K(z)$ 上合成). $F/K(z)$ 的Galois群同构于 $(\mathbb{Z}/2\mathbb{Z})^m$, $\tau \in \mathrm{Gal}(F/K(z))$ 的作用由 $\tau(\overline{s}_i) = \overline{s}_i$ 或 $\tau(\overline{s}_i) = \overline{s}_i + 1$ 给出. 此处 $\overline{s}_i$ 是 $\mathscr{F}$ 的第 i 个方程的左端在 F 中的一个根 $(0 \leqslant i \leqslant n-1)$.

证明 考虑 2 次 Artin-Schreier 算子 $\wp(x) = x^2 + x$ 及加法群 (或 $\mathbb{F}_2$ 模)

$$\Delta_0 = \mathrm{Span}_{\mathbb{F}_2}\{z^{-1} + \alpha_0 + \beta_0^{1/2}z, \cdots, z^{-1} + \alpha_{n-1} + \beta_{n-1}^{1/2}z\}.$$

定义 $\Delta = \Delta_0 + \wp(K(z))$, 则有 $F = K(z)\ (\wp^{-1}(\Delta)) = K(z)(\wp^{-1}(\Delta_0))$ 且

$$m = \dim_{\mathbb{F}_2}\big(\Delta/\wp(K(z)\big) = \dim_{\mathbb{F}_2}\big(\Delta_0/\Delta_0 \cap \wp(K(z))\big).$$

此处第 1 个等号是由于定理 17.2, 而第 2 个等号由群的第 1 同构定理导出.

由于将 $\wp$ 应用到 $K(z)$ 的非常数函数时必定包含 z 的 2 次项, 而这并不在 Δ_0 中, 所以有 $\Delta_0 \cap \wp(K(z)) = \Delta_0 \cap \wp(K)$. 简记

$$U = \mathrm{Span}_{\mathbb{F}_2}\{(1, \beta_0^{1/2}), \cdots, (1, \beta_{n-1}^{1/2})\}.$$

定义从 Δ_0 到 U 的一个线性映射如下: 对任意 $\alpha \in \Delta_0$, 取 z^{-1} 和 z 的系数作为 K^2 中向量的第 1 和第 2 分量, 就得到 U 中的一个向量. 显然这是从 Δ_0 到 U 的满线性映射, 其核为 $\Delta_0 \cap K$. 但该核中每一个元素必定是偶数个 α_j 之和 (否则, 因特征为 2, 奇数个 $z^{-1} + \alpha_i + \beta_i^{1/2}z$ 之和的结果必定含有 z^{-1}, 不在 K 中).

下面证明偶数个 α_i 之和必具有形式 $v^2 + v$, $v \in \mathbb{F}_2(\alpha)$. 事实上, 对于多项式 $f(t) = \sum d_i t^i \in \mathbb{F}_2[t]$ 及 $\varepsilon \in K$, 定义

$$f(t)\varepsilon = \sum d_i \varepsilon^{2^i}.$$

于是 K 的加群 K^+ 按上述作用成为一个 $\mathbb{F}_2[t]$ 模. 而我们要证明的结果可以重新叙述如下: 对于 $f(t) \in \mathbb{F}_2[t]$, $f(1) = 0$, 存在一个适当的 $v \in \mathbb{F}_2(\alpha)$, 使得 $f(t)\alpha = (t+1)v$ (这是因为 $f(1) = 0$ 表明 $f(t)$ 中的项数是偶数个, 而 $f(t)\alpha = \sum d_i \alpha^{2^i} = \sum d_i \sigma^i(\alpha)$, σ 是 2 次 Frobenius). 但这是容易的: 由于 $f(1) = 0$, 故 $t + 1 | f(t)$, 取 $v = \frac{f(t)}{t+1}\alpha$ 即可. 由此有 $\Delta_0 \cap K = \Delta_0 \cap \wp(K)$, 但 $\Delta_0 \cap \wp(K) = \Delta_0 \cap \wp(K(z))$, 我们有

$$\Delta_0/\Delta_0 \cap \wp(K(z)) = \Delta_0/\Delta_0 \cap \wp(K) = \Delta_0/\Delta_0 \cap K \cong U,$$

因此, $m = \dim_{\mathbb{F}_2} U$, 这就是引理 17.3 中关于 m 的公式.

为了证明 K 是 F 的常数域, 注意到 $F = K(z)(\wp^{-1}(\Delta))$, 我们必须证明: $\Delta \cap K \subseteq \wp(K)$. 由于每一个 $u \in \Delta \cap K$ 模去 $\wp(K)$ 后均同余于偶数个 α_j 之和, 于是由前面的结论, 知 u 模去 $\wp(K)$ 后具有形式 $v^2 + v = \wp(v)(v \in \mathbb{F}_2(\alpha))$, 从而 $u \in \wp(K)$. 所以 K 在 F 中是代数闭的.

下面证明 F 是前 m 个域 F_i 在 $K(z)$ 上的合成域. 在 Δ_0 的定义中, 前 m 个项组成了 $\mathbb{F}_2$ 向量空间 Δ_0 的一组基. 这可如下看出: 若第 i 个项与前面的 j 项, $0 \leqslant j \leqslant i-1$ 相关, 则第 $i+1, i+2, \cdots$ 项亦如此, 因为第 $i+1, i+2, \cdots$ 项可通过将 σ 重复应用到第 i 项而得到, 因此 F 可通过将 $\mathscr{F}$ 左端的前 m 个方程的根邻接到 $K(z)$ 上而得到, 即 $F = F_0 \cdots F_{m-1}$ 是 $F_0, \cdots, F_{m-1}$ 在 $K(z)$ 上的合成域.

最后, 由定理 17.2 和 $[F : K(z)] = 2^m$, 有 $\mathrm{Gal}(F/K(z)) \cong (Z/2\mathbb{Z})^m$. 对于任意的 $\tau \in \mathrm{Gal}(F/K(z))$, τ 固定所有的 $z^{-1} + \alpha_i + \beta_i^{1/2} z$, 因此 τ 必定将 $s_i^2 + s_i + z^{-1} + \alpha_i + \beta_i^{1/2} z$ 的根映射到它的根. 这就完成了引理的证明.

现在, 将 $\mathscr{F}$ 的第 0 个方程分别加到第 $i = 1, 2, \cdots, m-1$ 个方程, 并令 $t_i = s_0 + s_i$, $\gamma_i = \alpha_0 + \alpha_i$, $\delta_i = \beta_0^{1/2} + \beta_i^{1/2}$, 就得到

$$t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad i = 1, 2, \cdots, m-1. \tag{17.9}$$

这些方程定义了 $K(z)$ 的扩张 L_i, 使得 $F = F_0 L$, $L = L_1 \cdots L_{m-1}$ 是 L_i 在 $K(z)$ 上的合成域. 下面研究域 L.

引理 17.4 *域 L 是 $K(z)$ 的一个 2^{m-1} 次的扩域, 它是一个有理函数域: $L = K(c)$, 生成元 c, 使得 $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$, 其中 $\lambda_i \in K$, 且 $\lambda_0, \lambda_{m-1} \neq 0$.*

证明 因为 $2[L : K] = [F : L][L : K(z)] = [F : K(z)] = 2^m$, 所以 $[L : K(z)] = 2^{m-1}$.

下面归纳地应用更进一步的信息到 (17.9) 式. 我们希望找出一个变量替换以获得如下形式的方程:

$$t_i^2 + t_i + \delta_i t_{i-1} + \gamma_i = 0, \quad i = 1, 2, \cdots, m-1, \tag{17.10}$$

其中 $t_0 = z$.

首先, 取 (17.9) 式的第 1 个方程 $(i = 1)$ 作为 (17.10) 式的第 1 个方程: 现在假定经过某些变换, 对 $j \in [2, \cdots, m-1]$, 有方程

$$\begin{aligned} t_i^2 + t_i + \delta_i t_{i-1} + \gamma_i = 0, \quad i = 1, \cdots, j-1, \\ t_i^2 + t_i + \delta_i z + \gamma_i = 0, \quad i = j, \cdots, m-1, \end{aligned} \tag{17.11}$$

这些方程定义了扩张 $L/K(z)$. 由于 m 的定义, 这些方程的左端必是不可约的, 又由于 K 在 F 中是代数闭的 (引理 17.3), 故 $\delta_i \neq 0$. 现在以 $t_j + (\delta_j/\delta_1)^{1/2} t_1$ 代替 t_j,

并利用上面 $i=1$ 时的方程, 得出

$$t_j^2+t_j+\left(\left(\frac{\delta_j}{\delta_1}\right)^{1/2}+\frac{\delta_j}{\delta_1}\right)t_1+\frac{\delta_j}{\delta_1}+\gamma_j=0,$$

仍写该方程 t_1 的系数为 δ_j, 常数项为 γ_j, 有

$$t_j^2+t_j+\delta_j t_1+\gamma_j=0.$$

对此方程做变量代换 $t_j\to t_j+(\delta_j/\delta_2)^{1/2}t_2$, 并利用 (17.11) 式中第 2 个方程, 有

$$t_j^2+t_j+\left(\left(\frac{\delta_j}{\delta_2}\right)^{1/2}+\frac{\delta_j}{\delta_2}\right)t_2+\frac{\delta_j}{\delta_2}\gamma_2+\gamma_j=0,$$

将上述方程对 $t_2,t_3,\cdots,t_{j-2}$ 做下去, 最终得到

$$t_j^2+t_j+\delta_j t_{j-1}+\gamma_j=0.$$

因此, 由归纳法, 就可通过变量替换得到 (17.10) 式. 由 (17.10) 式有

$$z=(t_1^2+t_1+\gamma_1)/\delta_1,\quad t_1=(t_2^2+t_2+\gamma_2)/\delta_2,\ \cdots,$$

得到

$$z=\lambda_{-1}+\sum_{i=0}^{m-1}\lambda_i c^{2^i},\quad c=t_{m-1},\quad \lambda_i\in K.$$

因为 $L/K(z)$ 是可分的且 $[L:K(z)]=2^{m-1}$, 故有 $\lambda_0,\lambda_{m-1}\neq 0$, 证毕.

下面希望计算有关的函数域的亏格, 为此需要下述结果:

定理 17.3 设 L/K 是特征 2 的一个有理代数函数域. 设 $u\in L$ 是满足如下条件的一个元素:

$$u\neq w^2+w,\ \forall w\in L.$$

令 $F=L(y)$, $y^2+y=u$. 对于 L 的一个位(place)P, 定义整数 m_P 如下:

$$m_P=\begin{cases}m, & \text{若存在 } z\in L, \text{使得 } v_P(u+(z^2+z))=-m<0 \text{ 且 } m\not\equiv 0 \pmod 2,\\ -1, & \text{若 } v_P(u+(z^2+z))\geqslant 0 \text{ 对某个 } z\in L.\end{cases}$$

如果存在 L 的至少一个位 Q, 使得 $m_Q>0$, 则 K 在 F 中是代数闭的, 且

$$g=\frac{1}{2}\Big(-2+\sum_P(m_P+1)\deg P\Big),$$

这里, g 是 F 的亏格.

证明参见文献 [57], 我们这里叙述的是其中的一种特例.

定理 17.4　*F/K 是常数域 K 上亏格为 2^{m-1} 或 $2^{m-1}-1$ 的超椭圆函数域.*

证明　K 是 F 的常数域可由引理 17.3 知. 而由引理 17.4 知 $F=F_0L$ 且 $[F:L]=2$. 又由引理 17.4 知 L 是 K 上的有理函数域, 结合 $[F:L]=2$ 便知 F 的超椭圆性.

下面需要证明 F/K 的亏格是 2^{m-1} 或 $2^{m-1}-1$. 由 L 和 F 的定义知, 为了从 L 获得 F, 需要将定义 $\mathscr{F}$ 的第 1 个方程的一个根邻接到 L 上去. 我们知道方程 (未知变量 s_0) 的常数项是

$$u=1/z+\alpha_0+\beta_0^{1/2}z\in L,$$

而由引理 17.4, z 是 c 的一个次数为 2^{m-1} 的多项式 (系数在 K 中). 因为这个多项式是可分的, 它在 $K[c]$ 中分解成重数为 1 的不可约多项式之积. 设 P 是有理函数域 L 中任何位于 $z=0$ 上的位, 即使得 $v_P(z)>0$ 的那些位 P, 则 $v_P(u)=-1$, 从而 $m_P=1$. 又易知

$$\sum_{v_P(z)=0}\deg P=2^{m-1}\quad(\text{因为 } L \text{ 是有理函数域}).$$

现在考虑 $L=K(c)$ 的次数赋值 ∞. 因为 $z=\lambda_{-1}+\sum_{i=0}^{m-1}\lambda_i c^{2^i}$, 存在 $\widetilde{u}$, $v\in K[c]$, 使得 $\beta_0^{1/2}z=\widetilde{u}+v^2+v$ 且 $\deg(\widetilde{u})\leqslant 1$ (多项式 v 可以通过利用形如 $(\lambda c)^{2^i}+(\lambda c)^{2^{i-1}}$ 的多项式来连续消去 z 的右端的首项而得到), 因此

$$v_\infty(u+v^2+v)\geqslant 1,$$

从而 $m_\infty=1$ 或 $m_\infty=-1$.

而对于 L 的其余位 P, 均有 $v_P(u)=0$, 从而 $m_P=-1$. 将定理 17.3 应用到我们的情形, 有

$$g=\frac{1}{2}\Big(-2+\sum_P(m_P+1)\deg P\Big)=2^{m-1}\text{或}2^{m-1}-1.$$

这就完成了定理的证明.

定理 17.4 告诉我们, 曲线 $\mathscr{F}/K$ 是亏格为 2^{m-1} 或 $2^{m-1}-1$ 的超椭圆曲线. 下面需要限制到一个更小的常数域, 这时我们将利用域 F 上的 Frobenius 自同构的存在性, 即下面的

引理 17.5　*K 在 k 上的Frobenius自同构 σ 可以扩充 (不惟一) 为 F 上一个 n 或 $2n$ 阶的 k 自同构, 仍记其为 σ. 有 $\mathscr{F}$ 的左端的根 $\overline{s}_i=\sigma^i(\overline{s}_0)$, 从而有 $\mathfrak{D}$ 的左端的根 $\overline{w}_i=\sigma^i(\overline{w}_0)$, 其中 $\overline{w}_i=x\overline{s}_i+\beta_i^{1/2}$, $0\leqslant i\leqslant n-1$.*

证明 Frobenius 自同构 σ 显然可扩充到 $K(x) = K(z)$ 上的一个 k 自同构：$\sigma(x) = x$ (分别 $\sigma(z) = z$). 现在 F 可以通过在 $K(z)$ 上连续邻接上 $\mathscr{F}$ 的左端的根 $\bar{s}_i$ $(0 \leqslant i \leqslant m-1)$ 而获得. 一旦这 m 个根邻接到 $K(z)$ 上, 则其余的根 $\bar{s}_i$ $(m \leqslant i \leqslant n-1)$ 已能在 F 中找到, 从而 σ 将可以在其上定义. 所以, 我们只要看 σ 在 $\bar{s}_i$ $(0 \leqslant i \leqslant m-1)$ 上如何定义. 对 $m = 1$, 只要令 $\sigma(\bar{s}_0) = \bar{s}_0$. 现设 $m > 1$ 且 $\sigma : K(z)(\bar{s}_0, \cdots, \bar{s}_{i-1}) \to F$ 已定义好, 其中 $0 \leqslant i < m-1$. 我们可以扩充 σ 到 $K(z)(\bar{s}_0, \cdots, \bar{s}_i)$ 如下：$\sigma(\bar{s}_i) = \bar{s}_{i+1}$. 这是因为 $\mathscr{F}$ 的第 i 个方程的左端在 $K(z)(\bar{s}_0, \cdots, \bar{s}_{i-1})$ 上是不可约的. 而将 σ 应用到 $z^{-1} + \alpha_i + \beta_i^{1/2} z$ 上得出 $z^{-1} + \alpha_{i+1} + \beta_{i+1}^{1/2} z$. 因此, 我们可以通过定义 $\sigma(\bar{s}_i)(0 \leqslant i \leqslant m-1)$ 而将 σ 扩充到整个 F 上. 任何在 F 上的这种 σ 的阶必为 n 的倍数 (因为 $K \subseteq F$ 并且 σ 在 K 上的阶为 n). 更进一步, $\sigma^n(\bar{s}_0) = \bar{s}_0$ 或 $\sigma^n(\bar{s}_0) = \bar{s}_0 + 1$ (因为 $\sigma^n(\bar{s}_0)$ 必为 $\mathscr{F}$ 的第 1 个方程的左端的一个根), 因此 σ 在 F 上阶必为 n 或 $2n$. 引理中关于根的关系的叙述是显然的. 证毕.

引理 17.6 *假设下面的条件成立:*

$(*)$ *或者 n 是奇数, 或者 $m = n$, 或者 $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha) = 0$,*

则可选取引理17.5中Frobenius自同构在 F 上的扩充 σ, 使得它在 F 上的阶正好是 n.

证明 从 Frobenius 自同构在 F 上的任意一个扩充 σ 开始, 我们将 F^+ 变为一个 $\mathbb{F}_2[t_\sigma]$ 模：对任意 $f(t_\sigma) = \sum d_i t_\sigma^i \in \mathbb{F}_2[t_\sigma]$, 定义 $f(t_\sigma)s = \sum d_i \sigma^i(s)$, $\forall s \in F$. 易知在此作用下, F^+ 成为一个 $\mathbb{F}_2[t_\sigma]$ 模. 作为一个 F^+ 的子群, K^+ 继承了这个 $\mathbb{F}_2[t_\sigma]$ 模结构, 它与引理 17.3 证明过程中给出的 K^+ 的 $\mathbb{F}_2[t]$ 模结构是谐调的 (在关系 $t_\sigma = t^r$, $r = \log_2 q$ 下).

令 $f_{\beta_0}(t_\sigma)$ 是使得 $f_{\beta_0}(t_\sigma)\beta_0 = 0$ 的最低次多项式, 并置

$$f(t_\sigma) = \begin{cases} f_{\beta_0}(t_\sigma), & \text{若 } \deg(f_{\beta_0}(t_\sigma)) \text{ 是偶数}, \\ (t_\sigma + 1) f_{\beta_0}(t_\sigma), & \text{否则}. \end{cases}$$

我们可以对 $\beta_0^{1/2}$ 类似定义两个多项式, 显然它们与上面的 f_{β_0} 和 f 是相等的. 由于 $(t_\sigma^n + 1)\beta_0 = 0$, 存在 $h(t_\sigma) \in \mathbb{F}_2[t_\sigma]$, 使得 $h(t_\sigma)f(t_\sigma) = t_\sigma^n + 1$, 从而

$$\left(f(t_\sigma)\bar{s}_0\right)^2 + f(t_\sigma)\bar{s}_0 = f(t_\sigma)(\bar{s}_0^2 + \bar{s}_0) = f(t_\sigma)(z^{-1} + \alpha_0 + \beta_0^{1/2} z) = f(t_\sigma)\alpha_0,$$

此处用到了 $f(t_\sigma)\beta_0^{1/2} = 0$ 及 $f(1) = 0$ (这两点均可由 f 的定义得出). 由于 $f(1) = 0$, 利用引理 17.3 证明过程中的讨论, 可以找到 $v \in K$, 使得 $v^2 + v = f(t_\sigma)\alpha_0$ (于是 $v + 1$ 亦满足此式), 从而有

$$\left(f(t_\sigma)\bar{s}_0\right)^2 + f(t_\sigma)\bar{s}_0 + v^2 + v = f(t_\sigma)\alpha_0 + f(t_\sigma)\alpha_0 = 0,$$

即

$$\big(f(t_\sigma)\overline{s}_0+v\big)\big(f(t_\sigma)\overline{s}_0+v+1\big)=0,$$

进而 $f(t_\sigma)\overline{s}_0+v\in\{0,1\}$. 现在如下选取所需要的扩充 σ: 若 $f(t_\sigma)\overline{s}_0+v=1$, 则我们用下面的 σ' 代替 σ: 对于 $0\leqslant i<m-1$, 令 $\sigma'(\overline{s}_i)=\sigma(\overline{s}_i)$, 而 $\sigma'(\overline{s}_{m-1})=\sigma(\overline{s}_{m-1})+1$. 另一方面, 由引理 17.3 及其证明过程易知 $\deg\big(f(t_\sigma)\big)=m$. 因而 $f(t_\sigma)$ 的首项是 t_σ^m, 但是 $\overline{s}_{m-1}=\sigma^{m-1}(\overline{s}_0)$, 于是用 σ' 代替 σ 后, 可以假定

$$f(t_\sigma)\overline{s}_0+v=0. \tag{17.12}$$

上式乘以 $h(t_\sigma)$ 得到

$$(t_\sigma^n+1)\overline{s}_0+h(t_\sigma)=0.$$

由此可知: σ 在 F 上的阶为 n 当且仅当 $h(t_\sigma)v=0$. 另一方面, 由引理 17.3 的证明及前面说的 K^+ 模结构的谐调性, 我们可以选取

$$v=\frac{f(t^r)}{t+1}\alpha_0 \quad 或 \quad v=\frac{f(t^r)}{t+1}\alpha_0+1,$$

而

$$h(t^r)\cdot\frac{f(t^r)}{t+1}\alpha_0=\frac{(t^{rn}+1)}{t+1}\alpha_0=\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0),$$

于是有

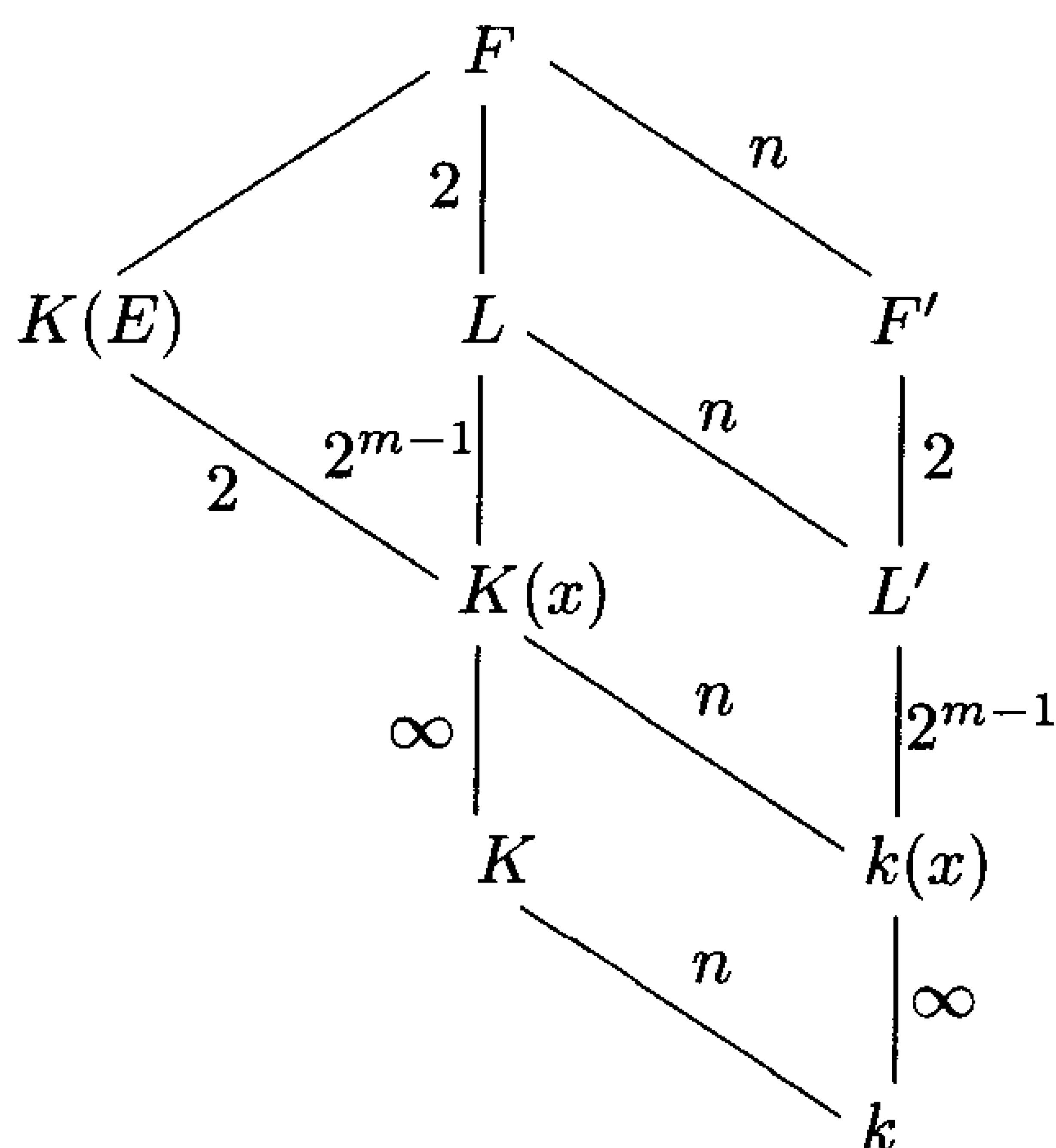
$$h(t_\sigma)v=\begin{cases}h(t^r)\cdot\dfrac{f(t^r)}{t+1}\alpha_0=\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0), & 或\\ h(t^r)\cdot\dfrac{f(t^r)}{t+1}\alpha_0+h(t^r)1=\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha_0)+h(1). &\end{cases} \tag{17.13}$$

而由前面可知, F 上的 k 自同构 σ (与 v 的选取有关) 的阶为 n 当且仅当 (17.13) 式右端至少一个为零. 而条件 (*) 就满足这样的要求: 情形 $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha)=0$ 是显然的. 若 n 为奇数, 则 $t_\sigma+1$ 只是 t_σ^n+1 的一重因子, 但 $t_\sigma+1|f(t_\sigma)$ 且 $h(t_\sigma)f(t_\sigma)=t_\sigma^n+1$, 所以 $h(1)=1$, 而当 $m=n$ 时, $h(t_\sigma)=1$, 从而 $h(1)=1$. 所以若 (*) 成立且 $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha)=1$, 则 (17.13) 式右端第 2 个式子 $\mathrm{Tr}_{K/\mathbb{F}_2}(\alpha)+h(1)=0$. 这就完成了引理的证明.

下面的定理给出了限制到更小的常数域时有关曲线的超椭圆性:

定理 17.5　*设 σ 是 K/k 的Frobenius到 F 的一个阶为 n 的扩充. 令 F' 是 σ 在 F 中的固定域, 即 $F'=\{f\in F\,|\,\sigma(f)=f\}$, 则 F' 是常数域 k 上的亏格为 2^{m-1} 或者 $2^{m-1}-1$ 的超椭圆函数域. 而曲线 $\mathscr{C}$ 有一个不可约的既约分支, 其函数域为 F'. 特别地, 如果条件 (*) 成立, 则这样的 k 自同构 σ 存在. 从而结论成立.*

证明　令 $L'=F'\cap L$, 则域 F, F', L 和 L' 之间关系如下:



由于 σ 在 F 上的阶为 n, 故 F' 在 F 中的指标为 n, 且由于 σ 在 K 上的阶为 n, 故 $F' \cap K = k$.

由于 L 是 F 的惟一指标为 2 的子域且 $K \subseteq L$, 故自同构 σ 限制到 L 上成一个 n 阶 k 自同构, 因此 $[L : L'] = n$ (因为 L' 是 σ 在 L 中的固定域, 而 σ 在 L 上的阶为 n), 从而 $[F' : L'] = 2$, 即证明了 F' 的超椭圆性. 又显然 $F = F'K$ 且 $L = L'K$, 结合定理 17.4, 便给出了有关亏格的叙述.

由引理 17.1 中的线性变换, 从 $\overline{w}_i$ 可得到 n 个元素 $\overline{y}_i$, 正如引理 17.1 所述, 自同构 σ 循环地作用在 $\overline{w}_i$ 上, 而固定所有 $\overline{y}_i$, 因此 $\overline{y}_i$ 属于 F', 加上 x, 它们就生成 F' (在 k 上) (因为 $\overline{w}_i$ 可由 K 上线性变换从 $\overline{y}_i$ 得出). 由引理 17.1, $\overline{y}_i$ 满足 $\mathscr{C}$ 的方程, 因此类似引理 17.2 中的证明, 知道 $\mathscr{C}$ 有一个不可约既约分支, 其函数域是 F'.

如果条件 (*) 成立, 则 σ 的存在性由引理 17.6 得出, 从而定理得证.

注记 17.1 若条件 (*) 不成立且 σ 的阶为 $2n$, 则在定理 17.5 的证明中我们得出 $F' = L'$, 因此不能保证找到定义在 k 上的曲线, 它有亏格 2^{m-1} 或 $2^{m-1} - 1$ 且是超椭圆的. 另一方面, 若设 $\#E(\mathbb{F}_{q^n}) = ph$, p 为一个大素数, $p \sim q^n$, 则 E 的 Weil 限制 A 同构于 $E(K)$ (作为群), 簇 A 包含一个不可约子簇 B, 其群阶可被 p 整除. 但 $p \sim q^n$, 通过简单的集合点数论证, 知该子簇 B 或为整个 A, 或者维数至少为 $n-1$. 我们希望找到 A 中的曲线 C, 其 Jacobian 含有一个同种于 B 的子簇, 这条曲线 C 最好是超椭圆的. 于是就可以对 C 来应用指标计算攻击法. 由于 Jac(C) 含有 B 的同种, 故 $g = \dim\mathrm{Jac}(C) \geqslant \dim(B) \geqslant n - 1$. 我们希望在定理 17.5 中构造出来的曲线 $\mathscr{C}$ 也就是这样的 C. 但是如果 m 太小, 则 $\mathscr{C}$ 的不可约分支的 Jacobian 不包含同种于 B 的子簇. 例如, 设 $E(\mathbb{F}_{q^n})$ 是一条 Koblitz 曲线, 即 E 定义在域 $\mathbb{F}_2$ 上, 则由 m

的定义, 将得到亏格 1 的 $\mathscr{C}$ 的不可约分支, 而此时 Weil 限制 A 的分解为乘积

$$A = E(\mathbb{F}_q) \times B_0,$$

此处 B_0 是定义在 $\mathbb{F}_q$ 上的 $n-1$ 维 Abel 簇. 而我们在定理 17.5 中构造的 Weil 限制中的曲线的不可约分支的 Jacobian 是同种于 $E(\mathbb{F}_q)$ 的, 因此我们不能从这些按定理 17.5 构造的曲线中得出关于子簇 B_0 的信息. 但这不意味着不能在 A 中找到有用的曲线, 其 Jacobian 含有同种于 B_0 的子簇. 这仅仅表明按照定理 17.5 构造的曲线不行. 这就是为何假定 E 不定义在 K 的真子域上的原因.

在本节剩下的部分, 总假定 K/k 的 Frobenius 自同构在 F 上有一个 n 阶的扩充 σ, 且 σ 循环地作用在 $\overline{s}_i$ 和 $\overline{w}_i$ 上, 而保持 x 和 z 不动. 例如, 条件 (*) 就是一个这样的充分条件.

下面我们希望获得定义 F/L 和 F'/L' 的 Atrin-Schreier 方程. 为了计算 F 在 L 上关于 s_0 和 c 的一个 Artin-Schreier 方程, 只要利用引理 17.4, 将 $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i}$ 代入 $\mathscr{F}$ 的第 1 个方程

$$s_0^2 + s_0 + z^{-1} + \alpha_0 + \beta_0^{1/2} z = 0$$

即可.

为了决定 σ 在 F 上的作用, 我们需要计算 $\sigma^i(c)$ 和 $\sigma^i(\overline{s}_0)(0 \leqslant i \leqslant n-1)$, 并将它们用 c 和 $\overline{s}_0$ 表示出来. 这可如下进行：由于

$$\begin{aligned} F = L(\overline{s}_0) = K(c)(\overline{s}_0) &= F_0 F_1 \cdots F_{m-1} \\ &= K(z)(\overline{s}_0, \overline{s}_1, \cdots, \overline{s}_{m-1}) \\ &= K(z)(\overline{s}_0, \sigma^1(\overline{s}_0), \cdots, \sigma^{m-1}(\overline{s}_0)), \end{aligned}$$

可见 $c \in K(z)(\overline{s}_0, \sigma^1(\overline{s}_0), \cdots, \sigma^{m-1}(\overline{s}_0))$, 从而 c 是 z 和 $\sigma^i(\overline{s}_0)(0 \leqslant i \leqslant m-1)$ 的 K 线性组合. 另一方面, 由上式也可知 $\sigma^i(\overline{s}_0) \in K(c)(\overline{s}_0)$, 而 $\overline{s}_0$ 在 $K(c)$ 上是 2 次的, 故存在 $f_i(c) \in K[c]$, 使得 $\sigma^i(\overline{s}_0) = f_i(c) + \overline{s}_0$, 从而 $\sigma^j(c)$ 是 z 和 $\sigma^i(\overline{s}_0)(0 \leqslant i \leqslant m-1)$ 的 K 线性组合, 从而可表示为 $\overline{s}_0$ 和 c 的多项式 (因为 $\sigma^i(\overline{s}_0) = f_i(c) + \overline{s}_0$, $z = \lambda_{-1} + \sum_{i=0}^{m-1} \lambda_i c^{2^i} = f(c)$).

给定 c 和 $\overline{s}_0$ 以及 σ 在 c 和 $\overline{s}_0$ 上的作用, 就可以如下清晰地构造出 F' 和 L':

定理 17.6　选取 $\mu \in K$, 使得 $\mathrm{Tr}_{K/k}(\mu) = 1$. 令 $\widetilde{c} = \mathrm{Tr}_{L/L'}(\mu\lambda_0 c)$, $\widetilde{s} = \mathrm{Tr}_{F/F'}(\mu\overline{s}_0)$, 则有 $L' = k(\widetilde{c})$ 且 $F' = k(\widetilde{s}, \widetilde{c})$, 而定义域扩张 F'/L' 的一个Artin-Schreier方程由下式给出：

$$\widetilde{s}^2 + \widetilde{s} + \frac{1}{z} + \mathrm{Tr}_{K/k}(\mu^2\alpha) + \mathrm{Tr}_{K/k}(\mu^2\beta^{1/2})z + \left(\mathrm{Tr}_{F/F'}(\mu^2\overline{s}_0) + \mathrm{Tr}_{F/F'}(\mu\overline{s}_0)\right) = 0,$$

其中上述方程左端 $\widetilde{s}$ 的系数和元素 z 及 $\mathrm{Tr}_{F/F'}(\mu^2\overline{s}_0) + \mathrm{Tr}_{F/F'}(\mu\overline{s}_0)$ 均在 L' 中.

证明 因为 $z=\lambda_{-1}+\sum_{i=0}^{m-1}\lambda_i c^{2^i}$ 和 $\sigma(z)=z$, 从扩域 $L/K(z)$ 的结构, 知 σ 将 c 的极点映到极点. 因为 $L=K(c)$ 是有理函数域, 故存在 $\lambda,\lambda'\in K$, 使得 $\sigma(c)=\lambda c+\lambda'$, 从而

$$\begin{aligned}\sigma(z)&=\sigma\Big(\lambda_{-1}+\sum\lambda_i c^{2^i}\Big)\\&=\sigma(\lambda_{-1})+\sum\sigma(\lambda_i)(\lambda'^{2^i}+\lambda^{2^i}c^{2^i}).\end{aligned}$$

但 $\sigma(z)=z$, 比较系数知, 对 $i\geqslant 0$, 有

$$\sigma(\lambda_i)\lambda^{2^i}=\lambda_i,$$

故对于 $i=0$, 有

$$\sigma(\lambda_0 c)=\sigma(\lambda_0)(\lambda c+\lambda')=\lambda_0 c+\sigma(\lambda_0)\lambda'.$$

因此, 利用上式可知

$$\widetilde{c}=\mathrm{Tr}_{L/L'}(\mu\lambda_0 c)=\lambda_0 c+\lambda'',\quad \lambda''\in K,$$

因此 $L'=k(\widetilde{c})$.

考虑 $\mathrm{Gal}(F/K(z))$, 由引理 17.3 知它是一个初等 Abel 2- 群, 其元素将每个 $\sigma^i(\overline{s}_0)$ 映到 $\sigma^i(\overline{s}_0)$ 或 $\sigma^i(\overline{s}_0)+1$. 现在令 τ 是 F/L 上的超椭圆对合, 它是 $\mathrm{Gal}(F/K(z))$ 的一个元素. 因为 τ 固定 L, 且任意一个 $\sigma^i(\overline{s}_0)$ 在 L 上生成 F, 必有 $\tau(\sigma^i(\overline{s}_0))=\sigma^i(\overline{s}_0)+1=\sigma^i(\tau(\overline{s}_0))$ 对一切 i 成立. 这表明 σ 和 τ 在 F 上的作用是可交换的, 从而 τ 可限制到 F'/L' 上 (因 F' 和 L' 的元素被 σ 固定). 再考虑定义 $\mathscr{F}$ 的方程. 由于 $\mathrm{Tr}_{K/k}(\mu)=1$, 故有 $\tau(\widetilde{s})=\widetilde{s}+1$, 从而

$$\mathrm{Tr}_{F'/L'}(\widetilde{s})=\widetilde{s}+\tau(\widetilde{s})=1.$$

再利用

$$\widetilde{s}^2=\mathrm{Tr}_{F/F'}(\mu^2\overline{s}_0^2)=\mathrm{Tr}_{F/F'}\big(\mu^2(\overline{s}_0+1/z+\alpha+\beta^{1/2}z)\big),$$

有

$$\begin{aligned}N_{F'/L'}(\widetilde{s})&=\widetilde{s}(\widetilde{s}+1)\\&=1/z+\mathrm{Tr}_{K/k}(\mu^2\alpha)+\mathrm{Tr}_{K/k}(\mu^2\beta^{1/2})z+\big(\mathrm{Tr}_{F/F'}(\mu^2\overline{s}_0)+\mathrm{Tr}_{F/F'}(\mu\overline{s}_0)\big).\end{aligned}$$

这就是定理 17.6 中的方程式. 这个方程关于 $\widetilde{s}$ 是可分的, 由构造知, 其系数在 L' 中 (因 $N_{F'/L'}(\widetilde{s})\in L'$, 而上式右端 $1/z+\mathrm{Tr}_{K/k}(\mu^2\alpha)+\mathrm{Tr}_{K/k}(\mu^2\beta^{1/2})z\in L'$, 故最后一项亦属于 L'). 由定义 $\mathscr{F}$ 的方程可知 $\overline{s}_i$ 在 z 的零点的赋值只有 $1/z$ 的赋值的一半, 而上式最后一项作为 L' 中元素, 是 $\overline{s}_i$ 的 K 线性组合, 因此除在 $\widetilde{c}=\infty$ 处外无极点, 从而是 $\widetilde{c}$ 的一个多项式, 因此可知定理 17.6 中的方程实际上是不可约的, 从而 $F'=k(\widetilde{s},\widetilde{c})$. 这就完成了定理的证明.

如第 1 节中所述, 将 E 上的离散对数问题变换成 F' 上的离散对数问题. 由于 F 是 $K(E)$ 和 F' 的函数域扩域, 因此, 有两个映射: 余范映射 $\mathrm{Con}_{F/K(E)}$ 和范映射

$N_{F/F'}$, 这两者均是除子群的同态. 它们将零次除子类映射为零次除子类, 由于椭圆曲线 E 的点群 $E(K)$ 与其函数域 $K(E)$ 的零次除子类群同构, 于是可将 $E(K)$ 中的离散对数问题如下转换: 首先将问题变换到 $Cl^\circ(K(E))$ 中, 由此利用 $\mathrm{Con}_{F/K(E)}$ 将其映射到 $Cl^\circ(F)$, 再利用 $N_{F/F'}$, 将其映入 $Cl^\circ(F')$, 将上述过程复合, 即有群同态

$$\phi: \ E(K) \longrightarrow Cl^\circ(F'),$$

我们需要的是 $E(K)$ 的大循环因子在此同态下保持不动.

引理 17.7　*映射 $\mathrm{Con}_{F/K(E)}: Cl^\circ(K(E)) \to Cl^\circ(F)$ 的核只能由 $Cl^\circ(K(E))$ 的 2 次幂扭元组成.*

证明　设 D 是 $K(E)$ 的零次除子, 由文献 [58] 中第 66 页, 知

$$N_{F/K(E)}\big(\mathrm{Con}_{F/K(E)}(D)\big) = [F : K(E)]D.$$

因此, 若 $\mathrm{Con}_{F/K(E)}(D)$ 是主除子, 则 $[F : K(E)]D$ 亦然. 但是 $[F : K(E)] = 2^{m-1}$, 这表明 $[D]$ 的阶为 2 的幂次, 证毕.

由上述引理可知, 如果 $E(K)$ 的大循环因子映射到零, 则它只可能是被 $N_{F/F'}$ 映到零的, 因为 $\phi = N_{F/F'} \circ \mathrm{Con}_{F/K(E)}$, 而 $\mathrm{Con}_{F/K(E)}$ 不能将大循环因子映到零.

现在设 P_1 和 $P_2 \in E(K)$, 欲解如下离散对数问题: 求 l, 使得

$$P_2 = [l]P_1.$$

利用 ϕ 将 P_i 映射到 $Cl^\circ(F')$ 中, 令 $D_i = \phi(P_i)$, 若并未得到 $D_1 = D_2 = 0$, 则可以试着在 $Cl^\circ(F')$ 中解这个离散对数问题. 这个问题可以利用超椭圆曲线离散对数的指标计算法来求解.

§17.3　奇特征的 GHS 攻击

在本节中, 固定以下记号: 设 K/k 是有限域的一个 n 次非平凡扩张, 其中 n 为奇数. $\overline{K}$ 记 K 的固定的代数闭包. H' 是 K 上的一条 (超) 椭圆曲线. 设 $K(H')$ 是 H' 的函数域, 固定某个嵌入 $K(x) \to K(H')$, 使得扩张 $K(H')/K(x)$ 的次数为 2 (对于 $g(H') \geqslant 2$, $K(H')$ 包含惟一的指标为 2 的有理子域, 而嵌入 $K(x) \to K(H')$ 惟一到 $K(x)$ 的一个同构). 固定 $K(x)$ 的一个可分闭包 $K(x)^{\mathrm{sep}}$ (包含 $K(H')$ 和 $\overline{K}(x)$), 以后将在此闭包中考虑问题. 若 $\widetilde{K}/K$ 是某个代数扩张, $\widetilde{K} \subseteq \overline{K}$, 则记合成域 $\widetilde{K}K(H')$ (在 $K(x)^{\mathrm{sep}}$ 中) 为 $\widetilde{K}(H')$.

记 $\sigma_{K/k}$ 为 K/k 的 Frobenius 自同构. 令 $\sigma_{K/k}(x) = x$, 则 $\sigma_{K/k}$ 扩充为 $K(x)/k(x)$ 的一个自同构, 仍记为 $\sigma_{K/k}$. 将 $\sigma_{K/k}$ 扩充成 $K(x)^{\mathrm{sep}}$ 的某个自同构 $\widehat{\sigma_{K/k}}$, 令 $\sigma^i_{K/k}(K(H'))$ 是 $K(H')$ 在 $\widehat{\sigma_{K/k}}^i$ 下的像. 注意 $K(H')/K(x)$ 是 Galois 扩张 (与 $\sigma_{K/k}$ 的扩张的选取无关). 令

$$F' = K(H')\sigma_{K/k}(K(H'))\cdots\sigma_{K/k}^{n-1}(K(H')), \tag{17.14}$$

它是 $K(H')/k(x)$ 的 Galois 闭包 (在 $k(x)^{\text{sep}}$ 内), 这一点可参见文献 [57]. 设 $m, \overline{m} \in \mathbb{N}$ 是如下定义的正整数:

$$[F' : K(x)] = 2^m, \quad [\overline{K}F' : \overline{K}(x)] = 2^{\overline{m}}. \tag{17.15}$$

设 k 是一个完备域 (perfect field), 如果 k 在函数域 F 中是代数闭的, 则称函数域 F/k 为正则的.

引理 17.8 *或者 F'/K 是正则的, 或者 F' 在 K 的惟一的二次扩域上是正则的.*

证明 设 $\widetilde{K}$ 是 K 在 F' 中的代数闭包, 则 $\text{Gal}(\widetilde{K}/K) \cong \text{Gal}(\widetilde{K}(x)/K(x))$. 这个群一方面是循环的, 另一方面又是 $\text{Gal}(F'/K(x))$ 的一个商群. 而 $\text{Gal}(F'/K(x))$ 同构于 $(\mathbb{Z}/2\mathbb{Z})^m$, 因此它仅有的循环商群是平凡的或 2 阶循环的. 引理证毕.

引理 17.9 *设 n 为奇数, 则 $K(x)$ 上的Frobenius映射 $\sigma_{K/k}$ 可扩充到 $F'/k(x)$ 的一个 n 阶自同构, 任意两个这样的扩充在 $\text{Gal}(F'/k(x))$ 中均是相互共轭的.*

证明 由 Galois 理论, 我们有下述短正合列:

$$1 \longrightarrow \text{Gal}(F'/K(x)) \longrightarrow \text{Gal}(F'/k(x)) \longrightarrow \text{Gal}(K(x)/k(x)) \longrightarrow 1,$$

这里 $\text{Gal}(K(x)/k(x)) \cong \text{Gal}(K/k)$. 群 $\text{Gal}(F'/K(x))$ 的阶 2^m 与 n 互素 (因假定 n 为奇数). 由两个熟知的 Zassenhaus 的群论定理, 上面的序列是分裂的, 因而两个断面必互相共轭 (参见文献 [59], I, 18.1, 18.2). 而我们的引理只不过是这个事实的另一种叙述.

固定 $\sigma_{K/k}$ 的一个扩充 $\widetilde{\sigma}_{K/k}$ 如引理 17.9 中所述, 并令 $F = F'^{\langle\widetilde{\sigma}_{K/k}\rangle}$ 是 $\widetilde{\sigma}_{K/k}$ 的固定域, 则 $[F' : F] = n$, $F' = KF$ 且 $F \cap K = k$.

若 F'/K 是正则的, 则 F/k 是正则的. 若 F'/K 不是正则的, 令 λ/k 是惟一的 2 次扩张, 则由引理 17.8, $F'/K\lambda$ 是正则的, 且 F/λ 是正则的 (见图 17.2).

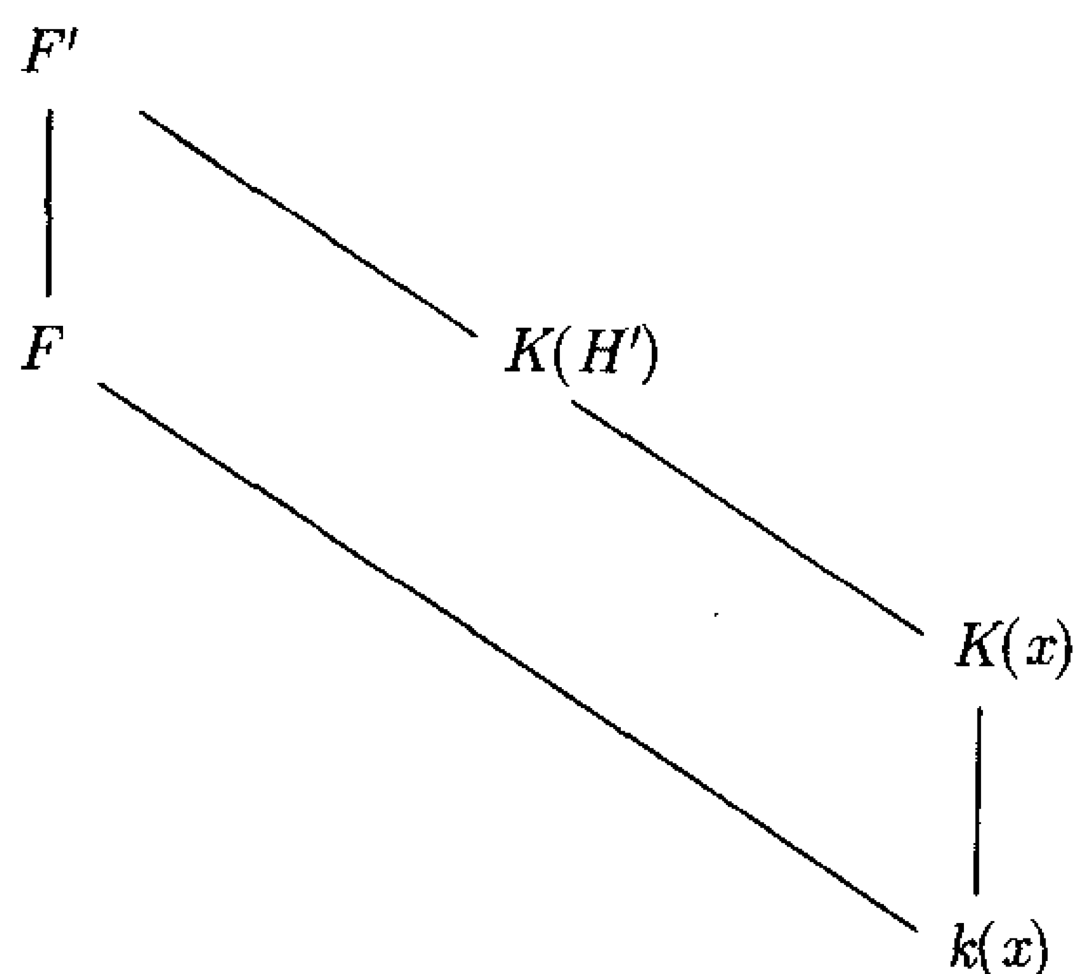


图 17.2

定理 17.7 设 F'/K 是正则的, 则存在 $F'/k(x)$ 的一个子扩张 $F/k(x)$, 使得 F/k 是正则的且 $KF=F'$, 且任意两个这种扩张 $F/k(x)$ 是同构的.

若 F'/K 不是正则的, 令 λ/k 是惟一的 2 次扩域, 则 $F'/\lambda K$ 是正则的且存在 $F'/\lambda(x)$ 的一个子扩张 $F/\lambda(x)$, 使得 F/λ 是正则的且 $\lambda KF=KF=F'$, 并且任意两个这样的扩张是同构的.

证明 需要证明定理中的任何扩张 $F_1/k(x)$ 或 $F_1/\lambda(x)$ 同构于前面构造的 $F/k(x)$ 或 $F/\lambda(x)$. 由于证明的类似性, 我们假定 F'/K 是正则的. 令 $F_1/k(x)$ 是 $F'/k(x)$ 的一个子扩张, 使得 F_1/k 正则且 $KF_1=F'$. F_1/k 是正则的等价于 $F_1\cap\overline{k}(x)=k(x)$, 特别地, $F_1\cap K(x)=k(x)$, 这表明限制同态

$$\mathrm{Gal}(F'/F_1)\longrightarrow\mathrm{Gal}(K(x)/k(x))$$

是一个同构. 因此 F'/F 和 F'/F_1 均是 n 阶的循环扩张, 并且存在生成元 $\alpha\in\mathrm{Gal}(F'/F_1)$, 使得 α 限制到 $\sigma_{K/k}\in\mathrm{Gal}(K(x)/k(x))$. 由引理 17.9, α 共轭于上面选取的 $\sigma_{K/k}$ 的扩张 $\widetilde{\sigma}_{K/k}$, 这表明 $F/k(x)$ 和 $F_1/k(x)$ 是同构的域扩张, 证毕.

下面考虑在何种情形下, 映射 (17.1) 的核不包含大素数阶的子群. 回顾映射 (17.1), 设 $K(H')$ 是 H' 的函数域, 则 $Cl^\circ(K(H'))=Cl^\circ(H')$. 令 $F'/K(H')$ 如 (17.14) 式中定义, 假设 F'/K 是正则的, 则由定理 17.7, 存在一个正则函数域 F/k, 使得 $KF=F'$. 于是有同态映射

$$N_{F'/F}\circ\mathrm{Con}_{F'/K(H')}:\quad Cl^\circ(K(H'))\longrightarrow Cl^\circ(F),\tag{17.16}$$

此处, $\mathrm{Con}_{F'/K(H')}$ 是余范映射, 而 $N_{F'/F}$ 是范映射, 这就是 (17.1) 式中的映射. 我们的想法如下: 若 $K(H')/k(x)$ 是 Galois 的, 则由 F' 的构造定义, 知 $F'=K(H')$, 从而 $KF=K(H')$, 进而在与密码学相关情形下, 素数阶大子群包含在 (17.16) 式 (即 (17.1) 式) 的核中. 因此, 为了保证核中不含大子群, 就应该使 $K(H')/k(x)$ 不是 Galois 的. 事实上有更强的条件: 没有 K/k 的中间域 μ 存在, 使得 $K(H')/\mu(x)$ 是 Galois 的. 即有

定理 17.8 设 K/k, H', F 和 F' 如定理17.7中, 假设不存在 K/k 的中间域 $\mu\subsetneq K$, 使得 $K(H')/\mu(x)$ 是Galois的, 则映射(17.1) (即(17.16)式) 的核只包含阶为 2 的幂次的元素.

为了证明这个定理, 我们需要下述引理:

引理 17.10 设 n 为奇数, μ 是 K/k 的中间域, 则下述 3 个条件等价:

1) $K(H')=\sigma_{K/\mu}(K(H'))$ (此处 $\sigma_{K/\mu}=\sigma_{K/k}^{[\mu:k]}$ 是 K/μ 的Frobenius);

2) $K(H')/\mu(x)$ 是Galois的;

3) 存在 2 次扩张 $M/\mu(x)$, 使得 M/μ 是正则的, 且 $KM=K(H')$.

证明 由于 $K(H')/\mu(x)$ 的 Galois 闭包是 $K(H')\sigma_{K/\mu}(K(H'))\cdots\sigma_{K/\mu}^{[K:\mu]-1}(K(H'))$, 故 1) 与 2) 的等价性是显然的.

又显然条件 3) 意味着前两个条件, 故假定 $K(H')/\mu(x)$ 是 Galois 的, 在定理 17.7 中, 以 K/μ 替代 K/k, 可知存在一个扩张 $M/\mu(x)$, 使得 M/μ 是正则的且 $KM=K(H')$. 由构造知 $M/\mu(x)$ 是 2 次扩张. 引理证毕

令 μ 是 K/k 的一个中间域, $\mu\subsetneq K$ 且引理 17.10 中条件成立. 令 $M/\mu(x)$ 如引理 17.10 中所述, 则映射 (17.16) 通过从 $Cl^\circ(K(H'))$ 到 $Cl^\circ(M)$ 的范同态分解. 事实上, 令 F_0' 是 $M/k(x)$ 的 Galois 闭包, 将引理 17.9 和定理 17.7 之间的推理应用到 μ/k, $M/k(x)$ 和 F_0', 存在扩张 $F_0/k(x)$, 使得 $\mu F_0=F_0'$, $F_0\cap\mu=k$. 现在令 λ 是 k 的惟一的 2 次扩张, 则取决于 F'/K 或 $F'/\lambda K$ 的正则性, 有 F_0/k 或 F_0/λ 的正则性. 更进一步, $F'=KF_0'=KF_0$, 因此, 由定理 17.7, $F_0/k(x)$ 同构于 $F/k(x)$ (特别地, F 包含在 $F_0'/k(x)$ 的 Galois 扩张中), 于是有下面的图表:

$$\begin{array}{ccc}
F'=KF_0 & & \\
| & \diagdown & \\
F_0'=\mu F_0 & & K(H')=KM \\
\| & \diagdown & | \\
F_0, F & & M
\end{array}$$

从而诱导出交换图表

$$\begin{array}{ccc}
Cl^\circ(F') & \longleftarrow & Cl^\circ(K(H')) \\
\downarrow & & \downarrow \\
Cl^\circ(\mu F_0) & \longleftarrow & Cl^\circ(M) \\
\downarrow & & \\
Cl^\circ(F) & &
\end{array}$$

其中水平方向是余范同态, 而垂直方向是范同态映射. 这表明映射 (17.16) 通过

$$N_{K(H')/M}:\ Cl^\circ(K(H'))\to Cl^\circ(M)$$

分解. 于是有

定理 17.9 设 μ 是 K/k 的中间域, 且 $K(H')/\mu(x)$ 是Galois的, 则存在一个正则函数域 M/μ, 使得 $KM=K(H')$, 且映射(17.16)通过 $N_{K(H')/M}:\ Cl^\circ(K(H'))\to Cl^\circ(M)$ 分解.

定理 17.9 实际上给出了 GHS 攻击失效的一个条件：设曲线 H' 是适合密码学应用的 (特别, $g(H') \leqslant 3$, $Cl^\circ(K(H'))$ 的阶是一个大素数与一个小因子之积), 假设存在一个如定理 17.9 中所述的域 $\mu \subsetneq K$, 则定理 17.9 表明映射 (17.16) 的核包含素数阶的大子群, 从而不能将 H' 上的离散对数问题按 GHS 方法转换成 $Cl^\circ(F)$ 中的相应问题.

定理 17.8 的证明　事实上, 我们将证明映射 (17.16) 的核被 2^{m-1} 零化, 即核中每个元素的阶都除尽 2^{m-1}. 首先固定一个记号, 设 $\alpha:\ A_1 \to A_2$ 是函数域的一个同态, 则以 $\underline{\alpha}$ 记从 $Cl^\circ(A_1)$ 到 $Cl^\circ(A_2)$ 的关于 α 的余范映射.

令 $l:\ K(H') \hookrightarrow F'$ 是包含映射, $\widetilde{\sigma}_{K/k}$ 是 $\sigma_{K/k}$ 到 $F'/k(x)$ 的一个固定的扩张, $F = F'^{\langle\widetilde{\sigma}_{K/k}\rangle}$, 则由定义知

$$\mathrm{Con}_{F'/K(H')} = \underline{l},$$

且

$$\mathrm{Con}_{F'/F} \circ N_{F'/F} \circ \mathrm{Con}_{F'/K(H')} = \sum_{i=0}^{n-1} \underline{\widetilde{\sigma}^i_{K/k}} \circ \underline{l}:\ Cl^\circ(K(H')) \longrightarrow Cl^\circ(F').$$

由于余范映射 $\mathrm{Con}_{F'/F}$ 是单的,

$$N_{F'/F} \circ \mathrm{Con}_{F'/K(H')}:\ Cl^\circ(K(H')) \longrightarrow Cl^\circ(F)$$

的核等于下述映射的核：

$$\sum_{i=0}^{n-1} \underline{\widetilde{\sigma}^i_{K/k}} \circ \underline{l}:\ Cl^\circ(K(H')) \longrightarrow Cl^\circ(F').$$

下面研究这个同态的核：

令 $\overline{\sigma^i_{K/k}}:\ K(H') \longrightarrow \sigma^i_{K/k}(K(H'))$ 是 $\widetilde{\sigma}^i_{K/k}$ 在 $K(H')$ 上的限制, 而 $l_i:\ \sigma^i_{K/k}(K(H')) \hookrightarrow F'$ 是包含映射, 则

$$\sum_{i=0}^{n-1} \underline{\widetilde{\sigma}^i_{K/k}} \circ \underline{l_i} = \sum_{i=0}^{n-1} \underline{l_i} \circ \underline{\overline{\sigma^i_{K/k}}}.$$

余范同态 $\underline{l_i}:\ Cl^\circ(\sigma^i_{K/k}(K(H'))) \to Cl^\circ(F')$ 诱导出一个同态

$$\bigoplus_i \underline{l_i}:\quad \bigoplus_{i=1}^{n-1} Cl^\circ(\sigma^i_{K/k}(K(H'))) \to Cl^\circ(F').$$

而余范同态 $\underline{\overline{\sigma^i_{K/k}}}:\ Cl^\circ(K(H')) \to Cl^\circ(\sigma^i_{K/k}(K(H')))$ 诱导出同态

$$(\underline{\overline{\sigma^i_{K/k}}})_i:\ Cl^\circ(K(H')) \longrightarrow \prod_{i=0}^{n-1} Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big) = \bigoplus_{i=1}^{n-1} Cl^\circ(\sigma^i_{K/k}(K(H'))).$$

复合上面这两个同态, 有

$$\sum_{i=0}^{n-1}\underline{\widetilde{\sigma}^i_{K/k}}\circ\underline{l}=\sum_{i=0}^{n-1}\underline{l_i}\circ\underline{\overline{\sigma^i_{K/k}}}=\Big(\bigoplus_i l_i\Big)\circ\Big(\underline{\overline{\sigma^i_{K/k}}}\Big)_i:\ Cl^\circ(K(H'))\longrightarrow Cl^\circ(F').$$

同态 $\Big(\underline{\overline{\sigma^i_{K/k}}}\Big)_i$ 显然是单的, 下面证明 $\bigoplus_i\underline{l_i}$ 的核的指数除尽 2^{m-1}. 范映射

$$N_i:=N_{F'/\sigma^i_{K/k}(K(H'))}:\ Cl^\circ(F')\longrightarrow Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big)$$

诱导出同态

$$\big(N_i\big)_i:\ Cl^\circ(F')\longrightarrow\prod_{i=0}^{n-1}Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big)=\bigoplus_{i=0}^{n-1}Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big).$$

我们将证明: $(N_i)_i\circ\big(\bigoplus_i\underline{l_i}\big)=2^{m-1}$ (特别地, 这表明 $\bigoplus_i\underline{l_i}$ 的核的指数除尽 2^{m-1}). 而这个事实可以从下面两个事实导出:

(a) 对 $i=0,1,\cdots,n-1$,

$$N_{F'/\sigma^i_{K/k}(K(H'))}\circ\mathrm{Con}_{F'/\sigma^i_{K/k}(K(H'))}:\ Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big)\longrightarrow Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big)$$

就是倍乘 2^{m-1}.

(b) 对于 $i,j=0,1,\cdots,n-1$, $i\neq j$,

$$N_{F'/\sigma^j_{K/k}(K(H'))}\circ\mathrm{Con}_{F'/\sigma^i_{K/k}(K(H'))}:\ Cl^\circ\big(\sigma^i_{K/k}(K(H'))\big)\longrightarrow Cl^\circ\big(\sigma^j_{K/k}(K(H'))\big)$$

是平凡的.

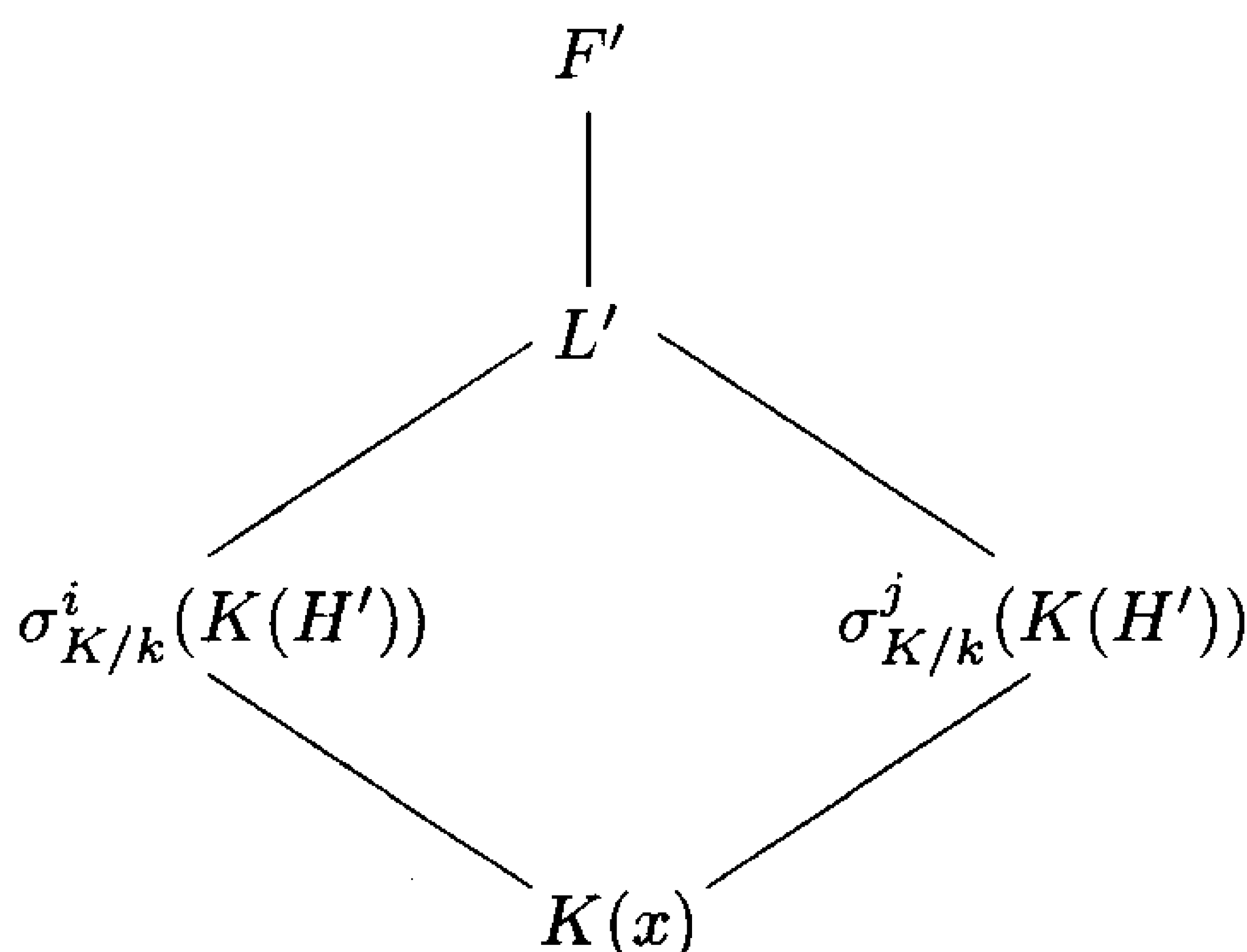
事实上, (a) 就是在证明引理 17.7 时引用过的结论. 我们来证明 (b).

由假设和引理 17.10 知: 不存在 $i=1,\cdots,n-1$, 使得 $K(H')=\sigma^i_{K/k}(K(H'))$, 从而不存在 $i,j=0,\cdots,n-1$, $i\neq j$, 使得 $\sigma^i_{K/k}(K(H'))=\sigma^j_{K/k}(K(H'))$.

设 $i\neq j$, $i,j\in\{0,1,\cdots,n-1\}$, 令

$$L'=\sigma^i_{K/k}(K(H'))\sigma^j_{K/k}(K(H')),$$

则 $L'/K(x)$ 是一个 4 次扩张, 而 F'/L' 是一个 2^{m-2} 次扩张.



我们有

$$
\begin{aligned}
& N_{F'/\sigma^j_{K/k}(K(H'))} \circ \mathrm{Con}_{F'/\sigma^i_{K/k}(K(H'))} \\
&= N_{L'/\sigma^j_{K/k}(K(H'))} \circ N_{F'/L'} \circ \mathrm{Con}_{F'/L'} \circ \mathrm{Con}_{L'/\sigma^i_{K/k}(K(H'))} \\
&= N_{L'/\sigma^j_{K/k}(K(H'))} \circ [2^{m-2}] \circ \mathrm{Con}_{L'/\sigma^i_{K/k}(K(H'))},
\end{aligned}
$$

此处 $[2^{m-2}]$ 记倍乘 2^{m-2}. 于是只要证明 $N_{L'/\sigma^j_{K/k}(K(H'))} \circ \mathrm{Con}_{L'/\sigma^i_{K/k}(K(H'))} = 0$ 即可. 而这可由下面的引理 17.11 导出.

$$
N_{L'/\sigma^j_{K/k}(K(H'))} \circ \mathrm{Con}_{L'/\sigma^i_{K/k}(K(H'))} = \mathrm{Con}_{\sigma^j_{K/k}(K(H'))/K(x)} \circ N_{\sigma^i_{K/k}(K(H'))/K(x)} = 0,
$$

因为 $Cl^\circ(K(x)) = 0$, 证毕.

引理 17.11　*设 A 是域 K 上的一个函数域, B/A 和 C/A 是有限Galois扩张, 而 BC 是 B 和 C 在 A 上的合成域, 使得在 BC 中有 $B \cap C = A$, 则*

$$
N_{BC/C} \circ \mathrm{Con}_{BC/B} = \mathrm{Con}_{C/A} \circ N_{B/A}: \quad Cl^\circ(B/K) \longrightarrow Cl^\circ(C/K).
$$

证明　引理显然可以由下述关于除子的事实得出:

$$
N_{BC/C} \circ \mathrm{Con}_{BC/B} = \mathrm{Con}_{C/A} \circ N_{B/A}: \quad \mathrm{Div}(B/K) \longrightarrow \mathrm{Div}(C/K).
$$

于是只要证明上述除子间映射的相等. 由于对除子群而言, 余范同态是单的, 故只要验证

$$
\mathrm{Con}_{BC/C} \circ N_{BC/C} \circ \mathrm{Con}_{BC/B} = \mathrm{Con}_{BC/C} \circ \mathrm{Con}_{C/A} \circ N_{B/A}:
$$

$$
\mathrm{Div}(B/K) \longrightarrow \mathrm{Div}(C/K).
$$

记对应于函数域同态 $\alpha: A_1 \to A_2$ 的除子群之间的余范映射仍为 α. 若 $\tau \in \mathrm{Gal}(BC/C)$, 记 τ 到 B 的限制为 $\overline{\tau}$, 记包含映射 $B \mapsto BC$ 为 l. 由关于合成域 BC/A 的假设, 知 $\mathrm{Gal}(BC/C) \to \mathrm{Gal}(B/A)$, $\tau \to \overline{\tau}$ 是一个同构 (参见文献 [60], VI, 定理 1.12) 且 $\tau l = l\overline{\tau}: B \to BC$.

对于除子 $D \in \mathrm{Div}(B/K)$, 有

$$
\begin{aligned}
& \mathrm{Con}_{BC/C} \circ N_{BC/C} \circ \mathrm{Con}_{BC/B}(D) \\
&= \sum_{\tau \in \mathrm{Gal}(BC/C)} \tau(l(D)) = l\Bigg(\sum_{\overline{\tau} \in \mathrm{Gal}(B/A)} \overline{\tau}(D)\Bigg) \\
&= \mathrm{Con}_{BC/B} \circ \mathrm{Con}_{B/A} \circ N_{B/A}(D) = \mathrm{Con}_{BC/A} \circ N_{B/A}(D) \\
&= \mathrm{Con}_{BC/C} \circ \mathrm{Con}_{C/A} \circ N_{B/A}(D).
\end{aligned}
$$

引理得证.

推论 17.1 设 n 为奇素数且 $K(H') \subsetneq F'$, 则映射(17.16) (即(17.1) 式)的核只含有阶为 2 的幂次的元素.

注记 17.2 在上面的讨论中, 我们并不需要对有限域的特征作任何假设, 所有结论对于奇特征均正确. 事实上, 这些结论推广了上一节的相应部分 (即对特征而言, 也对曲线而言, 我们未假定曲线是椭圆曲线, 它可以是超椭圆的). 另一方面, 只要假定定理 17.7 中的域 F 的存在性, 则定理 17.8 对 $n=[K:k]$ 为偶数亦成立.

下面假定有限域的特征为奇素数. 我们下面的目的是要计算函数域 $F' = K(H')\ \sigma_{K/k}(K(H'))\cdots\sigma_{K/k}^{n-1}(K(H'))$ 的亏格. 这与计算 $\overline{K}F'/\overline{K}$ 的亏格是一回事. 其次, 是想检测 F'/K 是否正则. 在第 1 节讨论这个问题时 (偶特征), 我们是利用 Artin-Schreier 理论. 现在, 对于奇特征情形, 需要用 Kummer 理论代替 Artin-Schreier 理论.

首先回顾一些所需的结果: 设 $\wedge$ 是一个域, 其特征不等于 2, 令 $\wedge^{\text{sep}}$ 是一个固定的可分闭包, 令 $\mu_2 \subseteq \wedge^*$ 是由 1 和 -1 组成的子群, 于是有下述对

$$\begin{array}{ccc}\mathrm{Gal}(\wedge^{\text{sep}}/\wedge)\times\wedge^* & \longrightarrow & \mu_2\\ (\sigma,u) & \longmapsto & \dfrac{\sigma(v)}{v},\end{array}$$

此处 $v^2=u$, $v\in\wedge^{\text{sep}}$. 设 U 是 $\wedge^*/\wedge^{*2}$ 的一个有限子群, 记 $\wedge[\sqrt[2]{U}]$ 是在 $\wedge$ 上由 U 中元素的平方根生成的子域, 则上面的对诱导出一个非退化的对

$$\langle *,*\rangle:\quad \mathrm{Gal}(\wedge[\sqrt[2]{U}]/\wedge)\times U\longrightarrow\mu_2, \tag{17.17}$$

这是指数 2 的有限 Abel 群之间的一个对. 将 U 视为一个 $\mathbb{F}_2$ 向量空间, 由于上面的对的非退化性, 有

$$[\wedge[\sqrt[2]{U}]:\wedge]=2^{\dim_{\mathbb{F}_2}U}. \tag{17.18}$$

同时, 上述对的非退化性还意味着下述:

引理 17.12 映射: $V\longmapsto\wedge[\sqrt[2]{V}]$ 给出了从 U 的子向量空间到 $\wedge[\sqrt[2]{U}]/\wedge$ 的子扩张之间的一个一一对应.

现在设 K 是一个完全域, $\mathrm{char}(K)\neq 2$. 固定一个代数闭包 $\overline{K}$ 和包含 $\overline{K}(x)$ 的可分闭包 $K(x)^{\text{sep}}$. 下面 $K(x)$ 的所有扩张均视为在 $K(x)^{\text{sep}}$ 之中. 现在将上面的结果应用到 $\wedge=K(x)$ 上. 为此, 首先固定下述记号: 若 $h\in K(x)^*$, 记 $\underline{h}$ 是 h 在 $K(x)^*/K(x)^{*2}$ 中的像. 设 $f_1,\cdots,f_n\in K(x)^*$, 令 $L_i/K(x)$ 是由 $y_i^2=f_i(x)$ 给出的扩张 (在 $K(x)^{\text{sep}}$ 中). 令 L 是 L_i 在 $K(x)^{\text{sep}}$ 中的合成域. 令 U 是由 $\underline{f_i}\in K(x)^*/K(x)^{*2}$ 生成的 $\mathbb{F}_2$ 向量空间, 而 $\overline{U}$ 是 U 在 $\overline{K}(x)^*/\overline{K}(x)^{*2}$ 中的像, 则 $L=K(x)[\sqrt[2]{U}]$, $\overline{K}L=\overline{K}(x)[\sqrt[2]{\overline{U}}]$.

引理 17.13 L/K 是正则的当且仅当 $U\to\overline{U}$ 是一个同构.

证明 L/K 是正则的当且仅当 $[L:K(x)]=[\overline{K}L:\overline{K}(x)]$. 由 (17.18) 式, 这等价于 $U\cong\overline{U}$. 引理得证

特别地, 有

引理 17.14 *设所有 f_i 是首一的, 则 L/K 是正则的.*

证明 由于 f_i 是首一的, 故 U 的所有元素均是首一的有理函数的像. 现在, 若 K 的一个首一有理函数在 $\overline{K}(x)$ 中是一个完全平方, 则它在 $K(x)$ 中已是一个完全平方 (因为 $\overline{K}/K$ 是可分的), 从而 $U\to\overline{U}$ 是同构的, 进而 L/K 是正则的, 证毕.

下面研究 $L/K(x)$ 的分歧情形.

引理 17.15 *$L/K(x)$ 在 $K(x)/K$ 的一个位 $\wp$ 是分歧的, 当且仅当存在一个 i, 使得 $L_i/K(x)$ 是分歧的. 若如此, 则 $\wp$ 在 $L/K(x)$ 中的分歧指标为 2.*

证明 这是 Abhyankar 引理的一个特殊情形, 请参见文献 [57], 命题 III. 8.9.

令 $\mathfrak{K}$ 是 K 在 L 中的代数闭包. 欲计算函数域 $L/\mathfrak{K}$ 的亏格. 由于亏格在常数域扩张下是不变的, 所以只要计算 $\overline{K}L/\overline{K}$ 的亏格即可.

设 r 是 $\overline{K}(x)/\overline{K}$ 中那些在至少 1 个 $\overline{K}L_i/\overline{K}(x)$ 中分歧的位的数目. 由引理 17.15, r 等于 $\overline{K}L/\overline{K}(x)$ 中那些分歧的位的数目. 令

$$\overline{m}:=\dim_{\mathbb{F}_2}(\overline{U}),\tag{17.19}$$

则由 (17.18) 式和 $[\overline{K}L:\overline{K}(x)]=2^{\overline{m}}$, 利用 Hurwitz 亏格公式, 有

$$g(L/\mathfrak{K})=g(\overline{K}L/\overline{K})=2^{\overline{m}}(0-1)+\frac{1}{2}r(2-1)\frac{2^{\overline{m}}}{2}+1=2^{\overline{m}-2}(r-4)+1.\tag{17.20}$$

若 $\overline{m}\geqslant 3$, $g(L/\mathfrak{K})=g(\overline{K}L/\overline{K})$ 是奇数, 特别地有

引理 17.16 *若 $\overline{m}\geqslant 3$, 则 $L/\mathfrak{K}$ 不是一个有理函数域.*

将引理 17.16 应用到 $\overline{K}L/\overline{K}(x)$ 的子扩张 (由引理 17.12, 这种子扩张均具有形式 $\overline{K}(x)[\sqrt[2]{\overline{V}}]$, $\overline{V}$ 是 $\overline{U}$ 的向量子空间), 若 $\overline{m}\geqslant 4$, 则 $\overline{K}L/\overline{K}(x)$ 不包含指标 2 的有理子域, 从而有

引理 17.17 *若 $\overline{m}\geqslant 4$, 则 $L/K(x)$ 不包含指标 2 的有理子域.*

证明 设 $M/K(x)$ 是一个指标 2 的子域, 则或者 $\overline{K}L/\overline{K}M$ 是次数 2 的扩张, 或者它是平凡的, 无论如何, 有 $g(\overline{K}M/\overline{K})\geqslant 1$. 证毕

为了下面进一步的讨论, 我们更清晰地描述 $K(x)^*/K(x)^{*2}$. 设 P 是 K 上首一不可约多项式的集合, 则 $K[X]$ 中的惟一分解定理诱导出一个同构

$$\begin{aligned}K^*\oplus\bigoplus_{p\in P}\mathbb{Z}&\xrightarrow{\ \sim\ }K(x)^*,\\(c,(f_p)_{p\in P})&\longrightarrow c\prod_{p\in P}p^{f_p}.\end{aligned}$$

因此, 有同构

$$K^*/K^{*2} \oplus \bigoplus_{p\in P} \mathbb{F}_2 \xrightarrow{\sim} K(x)^*/K(x)^{*2}, \tag{17.21}$$

注意, 若 K 是有限的 ($\mathrm{char}(K) \neq 2$), 则 $K^*/K^{*2} \simeq \mathbb{F}_2$.

下面考虑 GHS 攻击. 设 k 是奇特征有限域, K/k 是 n 次扩张 (n 为奇数), H' 是亏格 g 的一条 (超) 椭圆曲线, 而 $K(H')/K(x)$ 是一个 2 次扩张. 与前面一样, 令 F' 是 $K(H')/k(x)$ 在 $K(x)^{\mathrm{sep}}$ 中的 Galois 闭包. 由定理 17.9 和 17.8, 为了使 GHS 攻击有可能成功, 我们要假设: 不存在 K/k 的中间域 μ, 使得 $\mu \subsetneq K$ 且 $K(H')/\mu(x)$ 是 Galois 的.

扩张 $K(H')/K(x)$ 由 Weierstras 型方程给出:

$$y^2 = cf(x),$$

f 是次数为 $2g+1$ 或 $2g+2$ 的首一无平方因子多项式, $c \in K^*$. 由 Kummer 理论, 我们可以通过乘上 K^{*2} 中的元素来改变 c. 由于 $K^*/K^{*2} \simeq \mathbb{F}_2 \simeq k^*/k^{*2}$, 故可以选取 $c \in k^*$. 现在设 $c \in k^*$, 于是 F' 在 $K(x)$ 上由 $y_0, \cdots, y_{n-1}$ 生成, 其中

$$y_i^2 = c\sigma_{K/k}^i(f)(x),$$

因此 $F' = K(x)[\sqrt[2]{U}]$, 其中 $U \subseteq K(x)^*/K(x)^{*2}$ 是由 $\sigma_{K/k}^i(f)$ 在 $K(x)^*/K(x)^{*2}$ 中的像 $\underline{\sigma_{K/k}^i(f)}$ 生成的向量子空间. 令 $\overline{U}$ 是 U 在 $\overline{K}(x)/\overline{K}(x)^{*2}$ 中的像, 则由 (17.18) 式知, (17.15) 式定义的数 m 和 $\overline{m}$ 可描述如下:

$$m = \dim_{\mathbb{F}_2} U, \quad \overline{m} = \dim_{\mathbb{F}_2}(\overline{U}). \tag{17.22}$$

而引理 17.14 和定理 17.7 蕴含

定理 17.10　*若 $c=1$, 则 F'/K 是正则的, 且 F/k 亦是正则的.*

令 $\sigma_k \in \mathrm{Gal}(\overline{K}/k) \simeq \mathrm{Gal}(\overline{K}(x)/k(x))$ 是相对于 k 的 Frobenius 自同构, 类似于 $\sigma_{K/k}^i(K(H'))$, 定义 $\sigma_k^i(\overline{K}(H'))$, 则 $\sigma_k^i(\overline{K}(H'))$ 等于合成域 $\overline{K}\sigma_{K/k}^i(K(H'))$. 更进一步,

$$\overline{K}F' = \overline{K}(H')\sigma_k(\overline{K}(H'))\cdots\sigma_k^{n-1}(\overline{K}(H')).$$

现在想知道在哪些位上 $\overline{K}F'/\overline{K}(x)$ 是分歧的. 由引理 17.15, 这等于问 $\overline{K}(x)/\overline{K}$ 的哪些位在至少 1 个扩张 $\sigma_k^i(\overline{K}(H'))/\overline{K}(x)$ 中是分歧的.

将 $\overline{K}(x)/\overline{K}$ 的位与 $\overline{P} \cup \{\infty\}$ 等同起来, 其中 $\overline{P}$ 是 $\overline{K}$ 上的首一线性多项式的集合. Frobenius σ_k 作用在位上, 而这个作用对应于 σ_k 在 $\overline{P} \cup \{\infty\}$ 上的作用 (置 $\sigma_k(\infty) = \infty$).

扩张 $\overline{K}(H')/\overline{K}(x)$ 在某个 $p\in\overline{P}$ 是分歧的, 当且仅当 p 除尽 f, 而它在 ∞ 分歧当且仅当 $\deg(f)=2g+1$. 令 R 是 $\overline{K}(H')/\overline{K}(x)$ 的分歧位的集合, 即有 $\#R=2g+2$, 则 $\sigma_k^i(\overline{K}(H'))/\overline{K}(x)$ 正好在 $\sigma_k^i(R)$ 分歧, 而 $\overline{K}F'/\overline{K}(x)$ 正好在 $\bigcup_{i=0}^{n-1}\sigma_k^i(R)$ 分歧. 令

$$r:=\#\bigcup_{i=0}^{n-1}\sigma_k^i(R)$$

是 $\overline{K}F'/\overline{K}(x)$ 的分歧位的数目. 由 (17.20) 式, 有

$$g(F)=g(F')=2^{\overline{m}-2}(r-4)+1, \tag{17.23}$$

由 (17.22) 式知 $\overline{m}\leqslant n$, 而 $r\leqslant n\#R=n(2g+2)$, 从而

$$g(F)\leqslant 2^{n-2}((2g+2)n-4)+1=2^{n-1}((g+1)n-2)+1. \tag{17.24}$$

下面计算 $g(F)$ 的下界:

对于 $h\in K(x)^*$, 记它在 $K(x)^*/K(x)^{*2}$ 中的像为 $\underline{h}$, 对于 $h\in\overline{K}(x)^*$, 记它在 $\overline{K}(x)/\overline{K}(x)^{*2}$ 中的像为 $\overline{h}$. 因为 $\overline{U}$ 是 $\overline{m}$ 维的, 存在 $i_l(l=1,2,\cdots,\overline{m})$, 使得 $\overline{\sigma_{K/k}^{i_l}(f)}$ 形成 $\overline{U}$ 的一组基. 于是特别地有

$$\bigcup_{i=0}^{n-1}\sigma_k^i(R)=\bigcup_{l=1}^{\overline{m}}\sigma_k^{i_l}(R),$$

从而有

$$r=\#\bigcup_{l=1}^{\overline{m}}\sigma_k^{i_l}(R)\leqslant\overline{m}\#R=\overline{m}(2g+2).$$

进而

$$\overline{m}\geqslant\left\lceil\frac{r}{2g+2}\right\rceil. \tag{17.25}$$

群 $\mathrm{Gal}(\overline{K}/k)$ 作用在 $\bigcup_{i=0}^{n-1}\sigma_k^i(R)$ 上, 令 $\mathrm{Gal}(\overline{K}/\Delta)$ 是同态

$$\mathrm{Gal}(\overline{K}/k)\longrightarrow\mathrm{Aut}\Big(\bigcup_{i=0}^{n-1}\sigma_k^i(R)\Big)$$

的核.

引理 17.18 $K\subseteq\Delta$.

证明 只要证明 $K=K\cap\Delta$ 即可. 我们有

$$\mathrm{Gal}(\overline{K}/K\cap\Delta)=\langle\mathrm{Gal}(\overline{K}/K)\cup\mathrm{Gal}(\overline{K}/\Delta)\rangle.$$

而多项式 cf 被群 $\mathrm{Gal}(\overline{K}/k)$ 和 $\mathrm{Gal}(\overline{K}/\Delta)$ 固定, 从而 cf 被 $\mathrm{Gal}(\overline{K}/k\cap\Delta)$ 固定, $cf\in K\cap\Delta$, 这意味着 $K(H')/(K\cap\Delta)(x)$ 是 Galois 的. 但由于我们假定不存在中间域 μ, 使得 $\mu\subsetneq K$ 且 $K(H')/\mu(x)$ 是 Galois 的, 从而必有 $K\cap\Delta=K$. 证毕.

由 Δ 的定义, 我们有单同态

$$\mathrm{Gal}(\Delta/k)\longmapsto \mathrm{Aut}\Big(\bigcup_{i=0}^{n-1}\sigma_k^i(R)\Big). \tag{17.26}$$

令 $\delta=[\Delta:k]=\prod p^{\delta_p}$ 是 δ 的素因子分解. 由 (17.26) 式知 δ 阶的循环群可嵌入到 r 个元素的对称群之中, 从而有

$$r\geqslant\sum_{p,\delta_p\neq0}p^{\delta_p}. \tag{17.27}$$

令 $n=\prod_p p^{n_p}$ 是 n 的素因子分解. 由引理 17.18, $n|\delta$, 因此对所有 p, 有 $n_p\leqslant\delta_p$, 从而由 (17.27) 式有

$$r\geqslant\sum_{p,\,n_p\neq0}p^{n_p}. \tag{17.28}$$

由 (17.23)、(17.25) 和 (17.28) 式, 有

$$g(F)\geqslant 2^{\lceil\frac{\sum p^{n_p}}{2g+2}\rceil-2}\Big(\sum p^{n_p}-4\Big)+1, \tag{17.29}$$

因此, 我们有下述.

定理 17.11 设 $\mathrm{char}(k)\neq2$, K/k 是 n 次 (n 是奇数) 扩张, $n=\prod p^{n_p}$, H' 是 K 上的亏格 g 的 (超) 椭圆曲线, 选取一个 2 次扩张 $K(H')/K(x)$, 它由一个形式

$$y^2=cf(x)\ (f\text{首一},\ c\in K^*)$$

的方程给出, 则由GHS攻击, 我们得到一个在 k 上正则, 或在 k 的惟一的 2 次扩域上正则的函数域 F, 以及一个 2^m 次扩张 $KF/K(H')(m\leqslant n)$, 和一个从 $Cl^\circ(K(H'))$ 到 $Cl^\circ(F)$ 的同态 ϕ, 它们具有以下性质:

(a) 若 $c=1$, 则 F/k 正则;

(b) $g(F)\leqslant2^{n-1}((g+1)n-2)+1$;

(c) 若存在某个中间域 $k\subseteq\mu\subsetneq K$, 使得 $K(H')/\mu(x)$ 是Galois的, 则存在正则函数域 M/μ, 使得 $KM=K(H')$ 且同态 ϕ 可通过 $N_{K(H')/M}:\ Cl^\circ(K(H'))\to Cl^\circ(M)$ 分解;

(d) 如果不存在(c)中的域 μ, 则 ϕ 的核仅含有阶为 2 的幂次的元素, 且

$$g(F)\geqslant 2^{\lceil\frac{\sum p^{n_p}}{2g+2}\rceil-2}\Big(\sum p^{n_p}-4\Big)+1; \tag{17.30}$$

(e) 令 $\overline{m}$ 如 (17.22) 式定义, 若 $\overline{m} \geqslant 4$, 则 $F'/K(x)$ 不包含指标 2 的一个有理子域.

注记 17.3　定理 17.11 (e) 给出了奇特征时 GHS 攻击与偶特征时 GHS 攻击的主要差异. 由引理 17.4, 知道: 若 H' 是特征 2 上有限域 K 上的一条椭圆曲线, 则总可以选取一个扩张 $K(H')/K(x)$, 使得 $F'/K(x)$ 有一个指标 2 的有理子域.

下面, 对 n 为奇素数的情形进行更详细的讨论. 继续假定 $K(H')/k(x)$ 不是 Galois 扩张, 即 $K(H') \subsetneq F'$(否则, GHS 攻击失效), 由 (17.30) 式, 有

$$g(F) \geqslant 2^{\lceil \frac{n}{2g+2} \rceil - 2}(n-4)+1.$$

我们知道, $\mathrm{Gal}(K/k) \simeq \mathrm{Gal}(K(x)/k(x))$ 在 $K(x)^*$ 上的作用限制到子群 $\langle K^* \cup K(x)^{*2} \rangle$ 上一个作用, 从而获得 $K(x)^*/\langle K^* \cup K(x)^{*2} \rangle$ 上的一个作用. 而最后这个群包含在 $\overline{K}(x)/\overline{K}(x)^{*2}$ 中, 并且 $\overline{U}$ 是 $K(x)^*/\langle K^* \cup K(x)^{*2} \rangle$ 的一个子群. $\mathrm{Gal}(K/k)$ 的作用诱导出 $\mathrm{Gal}(K/k)$ 在 $\overline{U}$ 上的一个非平凡的作用. 从而有群环 $\mathbb{F}_2[\mathrm{Gal}(K/k)]$ 在 $\overline{U}$ 上的一个非平凡的作用. 由构造, $\overline{U}$ 是 $\overline{f} \in \overline{K}(x)^*/\overline{K}(x)^{*2}$ 在 $\mathbb{F}_2[\mathrm{Gal}(K/k)]$ 的作用下的像. 由于 $\mathbb{F}_2[\mathrm{Gal}(K/k)] \simeq \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$, $\overline{U}$ 是一个循环 $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ 模 (具有非平凡的 $\mathbb{Z}/n\mathbb{Z}$ 作用).

对于一个自然数 n, 令 $\varphi_2(n)$ 是 2 模 n 的乘法阶, 即 $\varphi_2(n) = [\mathbb{F}_2[\zeta_n] : \mathbb{F}_2]$.

引理 17.19　设 n 是一个奇素数, 而 V 是一个循环 $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ 模, 则

$$\dim_{\mathbb{F}_2}(V) = t\varphi_2(n) \text{ 或 } \dim_{\mathbb{F}_2}(V) = 1 + t\varphi_2(n),$$

对某个 $t = 0, \cdots, \frac{n-1}{\varphi_2(n)}$. 若 $\mathbb{Z}/n\mathbb{Z}$ 的作用是非平凡的, 则 $t \geqslant 1$.

证明　令 $V = \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]v$, 对某个 $v \in V$, 记 $\mathrm{Ann}(v) \subset \mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ 是 v 的零化子, 则作为 $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]$ 模, V 同构于 $\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}]/\mathrm{Ann}(v)$. 另一方面, 有环的典范同构

$$\mathbb{F}_2[\mathbb{Z}/n\mathbb{Z}] \simeq \mathbb{F}_2[x]/(x^n-1) \simeq \mathbb{F}_2 \oplus \mathbb{F}_2[x]/(x^{n-1}+x^{n-2}+\cdots+x+1),$$

而环 $\mathbb{F}_2[x]/(x^{n-1}+\cdots+x+1)$ 同构于 $\mathbb{F}_2[\zeta_n]^{\frac{n-1}{\varphi_2(n)}}$, 于是得出引理中的维数公式, 证毕.

将引理 17.19 应用到 $\overline{U}$, 有

$$\overline{m} = t\varphi_2(n) \text{ 或 } \overline{m} = 1 + t\varphi_2(n), \tag{17.31}$$

其中 $t = 1, 2, \cdots, \frac{n-1}{\varphi_2(n)}$.

由于 $r \geqslant n$, (17.23) 和 (17.31) 式蕴含了

定理 17.12　设 n 为奇素数, 则除了下界(17.30)外, 还有下述下界:

$$g(F) \geqslant 2^{\varphi_2(n)-2}(n-4)+1. \tag{17.32}$$

下面设 $n \geqslant 11$ 为素数, $H' = E'$ 为一条 K 上的椭圆曲线, 我们想给出 $q^{g(F)} \sim \#Cl^\circ(F)$ 的下界. 由于 $k = \mathbb{F}_q$, $K = \mathbb{F}_{q^n}$, 于是 (17.30) 式给出

$$g(F) > 2^{\lceil \frac{n}{4} \rceil - 2}(n-4) > 2^{\lceil \frac{n}{4} \rceil - 2} \cdot \frac{n}{2} = 2^{\lceil \frac{n}{4} \rceil - 3} n.$$

令 $c = \log_2(q^n)$, 则

$$\log_2(q^{g(F)}) = \frac{g(F)c}{n} > 2^{\lceil \frac{n}{4} \rceil - 3} c.$$

特别地, 若 $n \geqslant 29$, 则 $\log_2(q^{g(F)}) > 32c$.

也可以利用 (17.32) 式来给出 $\log_2(q^{g(F)})$ 的估计:

n	$\phi_2(n)$	$g(F)$	$\log_2(q^{g(F)})$
11	10	$\geqslant 2^{10-2}(11-4)+1 = 1793$	$\geqslant 163c$
13	12	$\geqslant 2^{12-2}(13-4)+1 = 9217$	$\geqslant 709c$
17	8	$\geqslant 2^{8-2}(17-4)+1 = 833$	$\geqslant 49c$
19	18	$\geqslant 2^{18-2}(19-4)+1 = 983041$	$\geqslant 51739c$
23	11	$\geqslant 2^{11-2}(23-4)+1 = 9729$	$\geqslant 423c$
⋮	⋮	⋮	⋮

因此有

定理 17.13 *设 K/k 是一个 n(素数) 次扩张, $n \geqslant 11$, 而 $H' = E'$ 是 K 上一条椭圆曲线, 则由GHS攻击得出的曲线 F 满足*

$$\log_2(q^{g(F)}) \geqslant 32 \log_2(q^n) = 32c.$$

特别地, 若 $E'(K)$ 具有密码学尺度, 即 $\log_2(\#K) \geqslant 160$, 则

$$\log_2(q^{g(F)}) > 5000.$$

因此, $\#Cl^\circ(F) \approx 2^{5000}$. 这表明对 $n \geqslant 11$, GHS 诱导出的高亏格曲线的 $Cl^\circ(F)$ 十分巨大, 从而现有的指标攻击方法在 $Cl^\circ(F)$ 中失效. 于是可知 GHS 攻击目前对此类椭圆曲线无效 (除非对高亏格类群的 DLP 的算法取得突破性进展).

注记 17.4 对于偶特征而言, 若 E 为一椭圆曲线, 则由上一节中构造出来的 F 的亏格为 2^{m-1} 或 $2^{m-1}-1$. 另一方面, 与本节类似, 但用 Artin-Schreier 理论替代 Kummer 理论, 我们也可以证明

$$m = t\varphi_2(n) \text{ 或 } m = t\varphi_2(n) + 1,$$

其中 $1 \leqslant t \leqslant \frac{n-1}{\varphi_2(n)}$. 因此, F 的亏格大致上是 $2^{t\varphi_2(n)}$. 为了能使 GHS 攻击有可能最好地实现, 希望 $2^{t\varphi_2(n)}$ 不要太大 (亏格太高的话, 指标计算攻击效率很低), 而当 n

为 Mersenne 素数时就如此. 因为当 $n = 2^a - 1$ 为 Mersenne 素数时, $\varphi_2(n) = a$, 从而 $2^{\varphi_2(n)} = n+1$. 而在密码学尺度内最重要的 Mersenne 素数是: 3, 7, 31, 127; 其次是当 n 为 Fermat 素数时: 3, 5, 17, 257. 当 $n = 5$ 时, 最小可能获得的亏格为 7, 当 $n = 17$ 时, 最小可能亏格为 127, 当 $n = 257$ 时, 最小可能亏格为 32768. 而对于奇特征而言, 当 $n = 2, 3, 5, 7$ 时, Diem 证明了存在 K 上的椭圆曲线, 使得 $g(F) = n$. 因此, 我们有下面的提醒:

(a) 对于特征 2 而言, 如果 n 被 4, 5, 6, 7, 31, 127 除尽, 则 $\mathbb{F}_{2^n}$ 上的椭圆曲线是可能有危险的. 而若使用超椭圆曲线, 则 n 被 2, 3, 4, 5, 6, 7, 31, 127 除尽时是可能有危险的.

(b) 对于奇特征 p 而言, 若 n 被 4, 5 或 7 除尽, 则 $\mathbb{F}_{p^n}$ 上的椭圆曲线是可能有危险的. 若利用亏格 2 的超椭圆曲线, 则 n 被 2, 3 除尽时是有危险的, 而对亏格 3 的超椭圆曲线, 则 n 被 2, 3, 5 或 7 除尽时是危险的.

(c) 对于奇特征域 $\mathbb{F}_{p^n}$ 而言, 当绝对扩张次数 $n \geqslant 11$ 为素数时, GHS 攻击对 $\mathbb{F}_{p^n}$ 上的椭圆曲线密码体制不构成大的威胁 (除非大亏格曲线上的 DLP 问题的算法有突破性进展).

§17.4　Weil 限制与低次扩域上的椭圆曲线离散对数攻击

设 E 是 $\mathbb{F}_{p^n}$ 上的一条椭圆曲线, 其方程为

$$E:\quad y^2 = x^3 + ax + b.$$

设 $f(t)$ 是 $\mathbb{F}_p$ 上的 n 次不可约的首一多项式, 使得 $\mathbb{F}_{p^n} = \mathbb{F}_p[t]/(f(t))$. 由 Weil 限制的定义 (参见 §17.1), 可知 E 的 Weil 限制 A 可视为 $\mathbb{F}_p$ 中的如下元素组成的集合:

$$\begin{aligned}A = \{&(x_0, \cdots, x_{n-1}, y_0, \cdots, y_{n-1}) \in \mathbb{F}_p^{2n} | x = x_0 + x_1 t + \cdots + x_{n-1}t^{n-1}\text{和}y\\ &= y_0 + y_1 t + \cdots + y_{n-1}t^{n-1}\text{是}E\text{上一个点的坐标}\}.\end{aligned}$$

而 A 上的群运算是从 E 的群运算导出的, 从而 A 成为一个 n 维的 Abel 簇.

下面, 我们直接利用指标计算攻击方法到 A 上, 而不是像前面的 GHS 攻击方法 (将指标计算方法应用到在 A 中的某条超椭圆曲线上). 为此, 我们要选取 A 的点集的一个因子基 $\mathscr{F}$, 一个自然的选取就是

$$\mathscr{F} = \{(x_0, \cdots, x_{n-1}, y_0, \cdots, y_{n-1}) | x_1 = x_2 = \cdots = x_{n-1} = 0\}.$$

它正好对应于 E 上那些 x 坐标在 $\mathbb{F}_p$ 中的点 $\mathscr{F}'$:

$$\mathscr{F}' = \{P = (x, y) \in E | x \in \mathbb{F}_p\}.$$

以后我们将不再区分 $\mathscr{F}$ 和 $\mathscr{F}'$. 注意, 如果这样选取的 $\mathscr{F}$ 是可约的, 则需要另外选取, 例如取 $x_0 = x_2 = \cdots = x_{n-1} = 0$. 下面总假定上面选取的 $\mathscr{F}$ 是适当的, 于是 $\#\mathscr{F} \approx p$.

设 P 和 Q 是 A 上两个点, Q 是 P 的一个倍点, 我们的目标是计算 Q 关于 P 的离散对数, 由指标计算攻击的一般想法, 随机取 a 和 b, 使得 a 和 b 均不超过 P 的阶. 并令 $R = aP + bQ$, 然后试图将它在选取的因子基 $\mathscr{F}$ 上进行分解. 如果得到一个分解, 就作为一个关系存起来, 然后再重复上述过程, 直到得到的关系式的个数多于 $\mathscr{F}$ 的势, 则对这些关系进行线性消元, 就可产生一个 P 和 Q 之间的非平凡的线性组合, 其结果为 A 中的零元, 从而得出所求的离散对数.

假设 R 是 E 的一个点, 欲将 R 表为 n 个点 $P_1, \cdots, P_n \in \mathscr{F}$ 的和. 对于 E 中任意点 P, 令其 x 坐标为

$$x_P = x_{0,P} + x_{1,P}t + \cdots + x_{n-1,P}t^{n-1}.$$

为了讨论 R 可否表成 $\mathscr{F}$ 中一些点之和, 引进 Semaev 的求和多项式如下: 设 $E: y^2 = x^3 + ax + b$ 是一条椭圆曲线, 则 E 的 n 次求和多项式如下递归定义:

$$\begin{aligned} f_2(X_1, X_2) &= X_1 - X_2, \\ f_3(X_1, X_2, X_3) &= (X_1 - X_2)^2 X_3^2 - 2((X_1 + X_2)(X_1X_2 + a) + 2b)X_3 \\ &\quad + ((X_1X_2 - a)^2 - 4b(X_1 + X_2)). \end{aligned}$$

对 $n \geqslant 4$ 和 $1 \leqslant k \leqslant n-3$,

$$f_n(X_1, \cdots, X_n) = \mathrm{Res}_X(f_{n-k}(X_1, \cdots, X_{n-k-1}, X), f_{k+2}(X_{n-k}, \cdots, X_n, X)),$$

其中 Res_X 表示关于未知量 X 的结式.

定理 17.14 设 E/k 是一条椭圆曲线, $n \geqslant 2$ 为整数, f_n 是其 n 次求和多项式, 设 $x_1, \cdots, x_n$ 是 k 的代数闭包 $\overline{k}$ 中的 n 个元素, 则 $f_n(x_1, \cdots, x_n) = 0$ 当且仅当存在 $\overline{k}$ 中的 n 有序对 $(y_1, \cdots, y_n)$, 使得对所有 i, $P_i = (x_i, y_i) \in E$ 且

$$P_1 + \cdots + P_n = 0.$$

对于 $n \geqslant 3$, 多项式 f_n 是对称多项式, 关于每一个变量的次数均为 2^{n-2}.

证明见文献 [61].

由定理 17.14, R 是否可表为 n 个点 $P_1, \cdots, P_n$ 的和, 就等价于解方程

$$f_{n+1}(x_{P_1}, x_{P_2}, \cdots, x_{P_n}, x_R) = 0,$$

其中 x_R 是已知的, 而 x_{P_i} 未知. 将上述方程表达为关于 t 的多项式并模去 $f(t)$, 从而获得如下形式的一个多项式:

$$\sum_{i=0}^{n-1} \varphi_i(x_{0,P_1}, \cdots, x_{0,P_n})t^i = 0,$$

其中所有 t^i 的系数都要为零, 因而得到关于 n 个未定元 $x_{0,P_1}, \cdots, x_{0,P_n}$ 的 n 个方程. 将这 n 个方程组成一个方程组, 用 Buchberger 算法求解之: 由于方程组的对称性 (因 f_{n+1} 的对称性), 我们可用 x_{0,P_i} 的初等对称多项式 $e_1, \cdots, e_n$ 将 φ_i 表示出来.

于是得到 n 个变量 $e_1, \cdots, e_n$ 的 n 个方程的方程组, 方程组中每一个方程的总阶数不超过 2^{n-1}. 于是利用 Lexicographic Gröbner 基, 我们获得的多变量多项式关于 e_1 的次数一般将是 $2^{n(n-1)}$. 而 Buchberger 算法的复杂度是这个次数和 $\mathbb{F}_p$ 的大小 (即 $\log p$) 的多项式, 从而寻找根的算法复杂度也是 $2^{n(n-1)}$ 和 $\mathbb{F}_p$ 的大小的多项式.

下面, 计算分解一个 A 中点 P 成功的概率. 设 f 是如下定义的函数:

$$\begin{aligned} f: \quad \mathscr{F}^n/S_n &\longrightarrow A, \\ (P_1, \cdots, P_n) &\longmapsto P_1 + \cdots + P_n, \end{aligned}$$

其中 S_n 是 n 阶对称群. 显然, P 能够成功分解当且仅当 $f^{-1}(P)$ 非空. 于是 $f^{-1}(P)$ 中元素的期望数是

$$\sum_{P\in A} \frac{f^{-1}(P)}{\#A} = \frac{1}{\#A}\#\big(\mathscr{F}^n/S_n\big) \approx \frac{1}{p^n} \times (p^n/n!) = \frac{1}{n!}.$$

此处用到了以下事实: $\#A \approx p^n$, $\#\mathscr{F} \approx p$. 后者由 $\mathscr{F}$ 的定义知, 而前者由 Weil 定理知, 因此, 分解一个 A 中点 P 成功的概率是 $1/n!$.

于是我们知道, 找到一个关系式的平均计算复杂度是

$$n!\mathrm{poly}(2^{n(n-1)})\mathrm{poly}(\log p).$$

现在可以计算整个指标算法的复杂度如下: 点的分解可以在

$$\mathrm{poly}(\log p)\mathrm{poly}(2^{n(n-1)})$$

时间内完成, 而找到一个关系平均需要 $n!$ 次分解, 总共需要搜集 $O(p)$ 个关系式. 最后要 $O(p^2)$ 个运算解线性代数问题. 因此有

定理 17.15 设 n 是一个固定的整数, 而 p 是一个素数 (或素数幂), 则当 p 趋于无穷时, 存在一个指标算法, 它可以在 $O(p^2)$ 时间内 (省去了对数因子) 解决定义

在有限域 $\mathbb{F}_{p^n}$ 上的任意椭圆曲线的离散对数问题. 事实上, 利用Thériault的具有大素因子的指标算法, 可以获得一个时间复杂度为 $O(p^{2-\frac{4}{2n+1}})$ 的算法 (省去了对数因子).

设 A 是定义在有限域 $\mathbb{F}_q$ 上的一个 n 维 Abel 簇, 于是可以有 A 的一个稠密的 Zariski 开子空间到一个 $n+m$ 维仿射空间的清晰的嵌入, 换言之, 一个元素 $P \in A$ 将由 $n+m$ 个坐标表示:

$$P = (x_1, \cdots, x_n, y_1, \cdots, y_m),$$

其中 $x_i, y_i \in \mathbb{F}_q$, 这样的表示对 A 中几乎所有元素都是可能的 (除去一个可忽略的部分外). 更进一步, 假定对 $\overline{\mathbb{F}_q}$ 中 $x_1, \cdots, x_n$ 的每一个选择仅存在有限个 $\overline{\mathbb{F}_q}$ 中的有序组 $y_1, \cdots, y_m$, 使得这 $m+n$ 个坐标产生 A 中一个点. 具有这种性质的一个坐标系称为该簇的一个 Noether 正规化.

当 $\dim(A) = 1$ 时, A 是椭圆曲线, 我们可以取 x_1 是横坐标, 而 y_1 是纵坐标. 而除无穷远点外, 所有其余点均可用此两坐标表示. 当 A 是一条超椭圆曲线的 Jacobian 时, 可以取 x_i 是 Mumford 表示中第 1 多项式系数, 而 y_i 是第 2 多项式的系数. 此时, 可与前面类似, 定义因子基

$$\mathscr{F} = \{P \in A | P = (x_0, 0, \cdots, 0, y_1, \cdots, y_m), x_1, y_1, \cdots, y_m \in \mathbb{F}_q\}.$$

一般来说, $\mathscr{F}$ 的维数是 1, 因此它是一条曲线或曲线的并, 由于 $\mathscr{F}$ 是一个不可约簇与一些超平面的交, 一般地它是不可约的. 若不然, 我们可以将坐标做一个随机的线性变换再试行上述过程. 因此, 我们总假定 $\mathscr{F}$ 是不可约的曲线, 从而其势约等于 q. 与前面的分析完全一样, 知道 A 中一个点被成功分解的概率是 $1/n!$. 而对于 A 中一个点 P, 是否存在 $\mathscr{F}$ 中的点 $P_1, \cdots, P_n$, 使得

$$P = P_1 + P_2 + \cdots + P_n,$$

以及如何计算这些点, 也可类似前面的讨论: A 上的群运算由我们给出的坐标的有理分式定义, 因此存在 $n+m$ 个清晰的有理分式 $\varphi_1, \cdots, \varphi_{n+m}$, 使得

$$P_1 + \cdots + P_n = \big(\varphi_1(P_1, \cdots, P_n), \cdots, \varphi_{n_m}(P_1, \cdots, P_n)\big).$$

于是可写出这 $(n+m)$ 有序对等于 P 的方程, 同时写出所有描述这些点是在 A 上或 $\mathscr{F}$ 上这些事实的方程 (注意对任何 $P = (x_1, \cdots, x_n, y_1, \cdots, y_m) \in A$, x_i 和 y_j 之间满足定义 A 的方程, 类似地对 $\mathscr{F}$ 上的点, 还有更多要满足的方程). 这样, 我们得到一个方程组, 其方程数大于未知量的个数. 于是一般地, 这个方程组定义了一个零维簇, 在 $\overline{\mathbb{F}_q}$ 上只有有限个解.

对于一个给定的 P, 找出所有定义在 $\mathbb{F}_q$ 上的解可通过一个 Gröbner 基计算和一个多变量多项式的分解完成. 这个多项式的次数由上述方程组中所有方程所定义的理想的次数所界定, 而计算复杂度是 $\mathbb{F}_q$ 的尺度大小和方程组的某些参数 (本质上取决于定义 A 的方程的次数) 的多项式.

我们总共需要搜集 $O(q)$ 个关系式, 最后为了解所得出的线性代数问题, 需要 $O(q^2)$ 的计算量. 这样, 我们有:

定理 17.16 *设 n 是一个固定的整数, A 是定义在有限域 $\mathbb{F}_q$ 上的 n 维 Abel 簇, 则可以在 $O(q^2)$ 时间内解决 A 上的离散对数问题. 如果利用Thériault的大素因子方法, 可以在 $O(q^{2-\frac{4}{2n+1}})$ 时间内解决 A 上的离散对数问题 (本定理中忽略了对数因子和只与 n 相关的常数).*

将定理 17.16 应用到超椭圆曲线的 Jacobian, 有

定理 17.17 *设 n 是一个固定的整数, C 是定义在 $\mathbb{F}_{p^n}$ 上的亏格为 g 的超椭圆曲线, 则存在一个算法解决 $\mathrm{Jac}_{\mathbb{F}_{p^n}}(C)$ 中离散对数问题, 其计算复杂度为 $O(q^2)$(若利用Thériault的大素因子方法, 则为 $O(q^{2-\frac{4}{2ng+1}})$). 此外, 忽略了对数因子和只与 n 相关的常数.*

证明 C 的 Jacobian 的 Weil 限制是一个定义在 $\mathbb{F}_p$ 上的 ng 维 Abel 簇, 具有一个从 Mumford 表示继承来的清晰的群运算 (用坐标系表示出来), 于是由定理 17.16 知定理 17.17 成立.

注记 17.5 当 p 足够大时, 对 $n=3$, 定理 17.15 给出的复杂度为 $O(p^{\frac{10}{7}})$, 它好过 Pollard 的 ρ 方法复杂度 $O(p^{3/2})$. 但对于现今的密码学尺度而言, 定理 17.15 的方法比 Pollard 的 ρ 方法在实际上慢, 主要原因是分解过程太耗时.

注记 17.6 在定理 17.17 中取 $n=1$, 则此时的 Weil 限制就是 C 的 Jacobian 本身. 此时已经有了基于 C 上的除子分解的经典指标算法. 事实上, 该算法可视为定理 17.17 的特例: 首先做一点变换, 对于除子的 Mumford 表示, 以一数乘上第 1 个多项式使其常数项为 1(显然这只有当除子的支集不含有横坐标为零的点时才行). 因此, 除了一个可忽略的部分外, Jacobian 的任何除子可以用下述两个多项式描述:

$$\langle u_g x^g + u_{g-1}x^{g-1} + \cdots + u_1 g + 1, v_{g-1}x^{g-1} + \cdots + v_1 g + v_0 \rangle.$$

现在 u_1 和 v_j 分别是前面 x_i 和 y_j 的角色. 从而可以定义因子基 $\mathscr{F}$ 是下述除子的集合: $u_g = u_{g-1} = \cdots = u_2 = 0$. 因此, $\mathscr{F}$ 正好由那些支集正好为曲线上一个点的除子组成 (加上无穷远点), 这正好就是经典的指标算法中的因子基. 因此, 超椭圆曲线的 Jacobian 的经典指标算法是定理 17.16(或定理 17.17) 中一般 Abel 簇上指标算法的特例, 只是坐标选取好到可以免去 Gröbner 基计算.

注意: 对于 $n>1$ 和 $\mathbb{F}_{p^n}$ 上的超椭圆曲线 C, 选取与上面注记中相同的坐标和

因子基 $\mathscr{F}$: 使得 $u_g = u_{g-1} = \cdots = u_2 = 0$ 且 $u_1 \in \mathbb{F}_p$ 的除子的集合. 于是分解可由两步骤构成: 首先试图将 R 表为 n 个除子 $D_1, \cdots, D_n$ 之和, 其中 D_i 是所有 $u_i \in \mathbb{F}_p$ 的除子, 其次, 检测 D_i 是否光滑 (即其 u 多项式是否完全分裂). 例如, $\mathbb{F}_{p^2}$ 上的亏格为 2 的曲线, 其分解步骤就是可实现的. 因而, 此曲线的安全性大大弱于所期望的. 因为离散对数可在 $O(p^{15/9})$ 内计算出来, 其中 O 中常数在一个可实现的范围内.

注记: 利用代数几何的方法来解决离散对数问题的思想是由 G.Frey 提出的, 本章的主要内容的写作参考了以下文献: C.Diem, The GHS-attacks in odd characteristic, J. Ramanujan Math. Soc. 18:1~32, 2003; Gaudry, F. Hess and N.Smart, Constructive and destructive facts of Weil descent on elliptic curves, J. of Cryptology, 15:19–46, 2002.

第十八章　离散对数的代数数论攻击方法

在本章中, 我们将利用代数数论中的有关理论对离散对数问题进行攻击, 特别地, 数域的 Brauer 群和 Galois 上同调在我们的叙述中起着重要的作用. 而局部和整体类域论的有关知识也是理解本章的基础.

§18.1　Brauer 群和 Galois 上同调

定义 18.1　设 K 是一个域, 称环 A 是一个 K 代数, 如果 A 具有一个 K 向量空间的结构, 并且满足

$$(\lambda a)b = a(\lambda b) = \lambda(ab), \quad \forall a, b \in A,\ \lambda \in K.$$

若 A 是一个 K 代数, 则 A 作为 K 向量空间的维数称为 A 的维数; 若对任意 $0 \neq a \in A$, a 均是可逆的, 则 A 称为 K 上的斜域或可除代数 (skew field 或 division algebra); 一个 K 代数同态 f: $A \to B$ 是从 A 到 B 的 K 线性的环同态; 而环 A 的理想也称为 K 代数 A 的一个理想; 一个 K 代数 A 称作单的, 若 A 只含有两个理想 (0) 和 A.

定理 18.1 (Wedderburn 结构定理)　设 A 是一个有限维单的 K 代数, 则存在恰好一个正整数 n 及恰好一个 (在 K 代数同构意义下)K 上的斜域 D, 使得 $A \simeq M_n(D)$, 其中 $M_n(D)$ 表示 D 上的 n 维矩阵代数.

若 A 是一个环, B 是 A 的子环, 则定义 B 在 A 中的中心化子如下:

$$Z_A(B) = \{a \in A | ab = ba, \forall b \in B\},$$

特别地, 记 $Z(A) := Z_A(A)$ 是 A 的中心 (化子). 设 A 是一个 K 代数, 假定 $K \subset A$, 显然有 $K \subset Z(A)$. 若 $K = Z(A)$, 则称 A 是 K 上的一个中心代数. 下面的定理表明一个有限中心单代数 A 的自同构都是内自同构:

定理 18.2 (Skolem-Noether)　设 A 是 K 上的一个有限中心单代数, 则 A 上的每一个 K 代数自同构 ϕ: $A \simeq A$ 一定是一个内自同构, 即存在一个单位 $u \in A$, 使得

$$\phi(a) = uau^{-1}, \quad \forall a \in A.$$

给定两个 K 代数 A 和 B, 我们可以作张量积: $A \otimes_K B$. 易知 $A \otimes_K B$ 有单位元 $1 \otimes 1$, 其中乘法定义如下:

$$(a_1 \otimes b_1)(a_2 \otimes b_2) = a_1 a_2 \otimes b_1 b_2, \quad \forall a_1, a_2 \in A, b_1, b_2 \in B.$$

而 $A \otimes_K B$ 的中心是 $Z(A) \otimes_K Z(B)$. 于是知: 若 A 和 B 是中心 K 代数, 则 $A \otimes_K B$ 亦然.

设 A 和 B 是两个 K 代数, 如果存在 $r, s \in \mathbb{N}$, 使得

$$A \bigotimes_K M_r(K) \simeq B \bigotimes_K M_s(K),$$

则称 A 和 B 是等价的, 记为 $A \sim B$. 对任何 K 代数 A, 记 $[A]$ 为 A 所在的等价类, 即

$$[A] = \{B | B \sim A\}.$$

设 K 是一个域, 定义域 K 的 Brauer 群如下:

$$\mathrm{Br}(K) = \{[A] | A\text{是}K\text{上的有限中心单代数}\}.$$

$\mathrm{Br}(K)$ 中的乘法由张量积诱导: $[A] \times [B] = [A \otimes B]$. 易知这个乘法与代表元的选取无关. 显然 $\mathrm{Br}(K)$ 的单位元是 $[K]$, 而张量积的性质表明 $\mathrm{Br}(K)$ 中的乘法是结合和交换的. 为了说明 $\mathrm{Br}(K)$ 在此乘法下构成一个群, 只要再说明逆元的存在性. 设 A 为任意一个有限中心单代数, 令 A^{opp} 是 A 的反代数, 即作为 K 向量空间, 有 $A^{\mathrm{opp}} = A$, 但 A^{opp} 上的乘法定义如下:

$$A^{\mathrm{opp}} \times A^{\mathrm{opp}} \longrightarrow A^{\mathrm{opp}}, \quad a \times b \longmapsto ba,$$

其中 $a \times b$ 表示 A^{opp} 中乘法而 ba 表示 A 中乘法. 易知

$$[A] \times [A^{\mathrm{opp}}] = [K] = 1_{\mathrm{Br}(K)},$$

因此 $\mathrm{Br}(K)$ 是一个群.

设 L 是 K 的一个代数扩张, A 是一个 K 代数, 则 $A \otimes_K L$ 是一个 L 代数. 于是诱导出一个群同态

$$\mathrm{res}_{L/K}: \quad \mathrm{Br}(K) \longrightarrow \mathrm{Br}(L), \ [A] \longmapsto [A \bigotimes_K L],$$

若 $[A] \in \mathrm{Ker}(\mathrm{res}_{L/K})$, 则称 K 的扩张 L 是 A 的分裂域. 而称

$$\mathrm{Br}(L/K) := \mathrm{Ker}(\mathrm{res}_{L/K})$$

是 K 关于 L 的相对 Brauer 群.

引理 18.1　设 L/K 是 A 的一个分裂域, 这等价于存在一个包含 L 的代数 $\widetilde{A}$, 它等价于 A 且具有维数 $[L:K]^2$. 设 D 是 K 上的一个有限中心斜域, 而 L 是 D 的极大子域, 则 L/K 是 D 的一个分裂域且 $\dim_K(D)=[L:K]^2$.

设 A 是 K 上的一个有限中心单代数, 则存在 A 的一个分裂域 L/K, 它是 K 的有限 Galois 扩张. 因此 Brauer 群 $\mathrm{Br}(K)$ 可以借助相对 Brauer 群描述如下:

$$\mathrm{Br}(K)=\bigcup_{L/K\text{是有限 Galois}}\mathrm{Br}(L/K).$$

于是我们可以集中注意力来研究 $\mathrm{Br}(L/K)$, 其中 L/K 是有限 Galois 扩张.

定理 18.3　(i) 设 k 是有限域, 则 $\mathrm{Br}(k)=1$;

(ii) 设 K 是代数闭域, 则 $\mathrm{Br}(K)=1$;

(iii) 设 K 是实闭域, 则 $\mathrm{Br}(K)\cong\mathbb{Z}/2\mathbb{Z}$.

证明　设 A 是 k 上的任意一个有限中心单代数, 我们要证明 $[A]=[k]$. 但由 Wedderburn 结构定理, 有 k 上的一个斜域 D, 使得 A 同构于 $M_n(D)$. 下面将证明 $D=k$, 从而 $A\cong M_n(k)$, 于是有 A 与 k 等价 (因为存在 $r=1$, $s=n$, 使得 $A\bigotimes_k M_r(k)=A=M_n(k)=k\bigotimes_k M_s(k)$, 于是按定义 $A\sim k$), 即 $[A]=[k]$, 可见 $\mathrm{Br}(k)=1$. 下面证明 $D=k$.

设 D 是 k 上一个有限中心斜域, 则 D 的每一个元素均包含在 D 的一个极大子域之中, 但是由引理 18.1, 所有极大子域在 k 上的维数均为 $\sqrt{\dim_k(D)}$. 由于 k 是有限域, 故 k 的给定扩张次数的所有扩域都是 k 同构的. 于是所有这些极大子域均是相互同构的. Skolem-Noether 定理 18.2 告诉我们, 所有这些极大子域一定具有形式 xLx^{-1}, 其中 $x\in D^*=D\setminus\{0\}$, 而 L 是一个固定的极大子域, 因此

$$D^*=\bigcup_{x\in D^*}xL^*x^{-1}$$

(因为 D 中每个元素均包含在 D 的某个极大子域之中). 但是 D^* 和 L^* 均是有限群, 若一个有限群 G 是其子群 H 的所有共轭之并, 则 $G=H$, 从而 $D^*=L^*$, 于是 $D=L$, 故 D 是交换的. 由于 D 是 k 上的中心代数, 这表明 $D=k$, 这就证得 (i).

(ii) 与 (i) 的证明类似, 只要证明: 若 D 是 K 上一个有限可除代数, 则必有 $D=K$. 事实上, 设 E 是 D 的一个交换子代数, 则 E 是 K 上一个整环 (一个有单位元的交换的无零因子环), 由于 $\dim_K(E)\leqslant\dim_K(D)<+\infty$, 故 E 作为 K 向量空间是有限维的, 从而 E 在 K 上是代数的. 但是 K 是代数闭的, 于是 $E=K$. 现在, 对任意 $a\in D$, 考虑 D 的子代数 $K[a]$, 由前知 $K[a]=K$, 故 $a\in K[a]=K$, 因此 $a\in K$, 于是 $D=K$, 因此 $\mathrm{Br}(K)=1$.

(iii) 由 Frobenius 证明的一个定理, 知定义在一个实闭域 K 上的仅有的有限维真斜域只有 Hamilton 四元域. 这意味着有: $\mathrm{Br}(K)\cong\mathbb{Z}/2\mathbb{Z}$. 定理证毕.

定义 18.2 设 G 是一个有限群, M 是一个 Abel 群, G 作用在 M 上且满足以下 3 个条件:

(1) $1 \cdot a = a, \forall a \in M$;

(2) $\sigma(a+b) = \sigma a + \sigma b, \forall \sigma \in G, a, b \in M$;

(3) $(\sigma\tau)a = \sigma(\tau a), \forall \sigma, \tau \in G, a \in M$;

则称 M 是一个 G 模.

设 A 是一个 G 模, 令 A_q 是 q 上链的集合, 即 A_q 是映射

$$x: \underbrace{G \times \cdots \times G}_{q\text{个}} \longrightarrow A$$

的集合. 定义映射 $\partial_q: A_{q-1} \to A_q$ 如下:

$$(\partial_1 x)(\sigma) = \sigma x - x, \qquad \forall x \in A_0 = A$$

$$(\partial_q x)(\sigma_1, \cdots, \sigma_q) = \sigma_1 x(\sigma_2, \cdots, \sigma_q) + \sum_{i=1}^{q-1}(-1)^i x(\sigma_1, \cdots, \sigma_{i-1}, \sigma_{i+1}, \cdots, \sigma_q)$$
$$+ (-1)^q x(\sigma_1, \cdots, \sigma_{q-1}), \quad \forall x \in A_{q-1},\ q \geqslant 1.$$

易知, $\partial_{q+1} \circ \partial_q = 0$. 定义 q 上闭链 Z_q 和 q 上边缘 R_q 如下:

$$Z_q = \ker(\partial_{q+1}) \subset A_q, \quad R_q = \mathrm{Im}(\partial_q) \subset A_q.$$

由于 $\partial_{q+1} \circ \partial_q = 0$, 故有 $R_q \subset Z_q$. 于是有

定义 18.3 商群

$$H^q(G, A) = Z_q / R_q, \quad q \geqslant 1$$

称为 G 模 A 的 q 维上同调群, 对于 $q = 0$, 令 $H^0(G, A) = A^G = \{a \in A | \sigma a = a, \forall \sigma \in G\}$.

由于在算术应用中, 低维上同调群具有特殊的重要性, 所以我们给出低维上同调群的代数描述.

当 $q = 1$ 时, 1 上闭链是函数 $x: G \to A$, 满足 $\partial_2 x = 0$, 从而

$$x(\sigma\tau) = \sigma x(\tau) + x(\sigma), \quad \forall \sigma, \tau \in G.$$

因此, 1 上闭链就是所谓交叉同态. 而 1 上边缘则是如下函数:

$$x(\sigma) = \sigma a - a, \quad \sigma \in G,$$

对某个 $a \in A$. 如果 G 在 A 上的作用是平凡的, 则显然有

$$H^1(G, A) = \mathrm{Hom}(G, A).$$

当 $q=2$ 时, 2 上闭链是满足 $\partial_3 x=0$ 的函数, 因此有

$$x(\sigma\tau,\rho)+x(\sigma,\tau)=\sigma x(\tau,\rho)+x(\sigma,\tau\rho),\ \ \sigma,\tau,\rho\in G.$$

而 2 边缘则满足

$$x(\sigma,\tau)=\sigma y(\tau)-y(\sigma\tau)+y(\sigma),$$

其中 y 是某个 1 上链, $y:\ G\to A$.

下面的定理是上同调论中十分基本和重要的工具:

定理 18.4　设

$$0\longrightarrow A\stackrel{i}{\longrightarrow}B\stackrel{j}{\longrightarrow}C\longrightarrow 0$$

是 G 模的正合序列, 则有如下的长正合序列:

$$\begin{array}{ccccccc}0\longrightarrow & A^G & \stackrel{i_0}{\longrightarrow} & B^G & \stackrel{j_0}{\longrightarrow} & C^G & \\ \stackrel{\sigma_1}{\longrightarrow} & H^1(G,A) & \stackrel{i_1}{\longrightarrow} & H^1(G,B) & \stackrel{j_1}{\longrightarrow} & H^1(G,C) & \longrightarrow\cdots\end{array}$$

(*称之为正合上同调序列*).

此处 σ 映射具有如下清晰的描述: 设 $c_q\in H^q(G,C)$ 给定, 则可有一个 q 上闭链 C_q 表示 c_q, $C_q:\ G^q\to C$. 由于 $j:\ B\to C$ 是满的, 故可以找到一个 q 上链 B_q, 其值在 B 中, 且 $j(B_q)=C_q$. 于是有

$$0=\partial C_q=\partial j(B_q)=j(\partial B_q).$$

因此 B_q 是位于 j_{q+1} 的核中, 因此存在一个 $(q+1)$ 上闭链 A_{q+1}, 满足 $\partial B_q=i(A_{q+1})$. 现在, 有

$$0=\partial\partial B_q=\partial i(A_{q+1})=i(\partial A_{q+1}).$$

由于 i 是单射, 故 $\partial A_{q+1}=0$. 从而 A_{q+1} 是一个 $(q+1)$ 上闭链, 定义 $\sigma_q(C_q)$ 就是 A_{q+1} 在 $H^{q+1}(G,A)$ 中的类 a_{q+1}, 即 $\sigma_q(c_q)=a_{q+1}$.

设 K 是一个完全域 (perfect field), $\overline{K}$ 是 K 的一个代数闭包, 而 $G=\mathrm{Gal}(\overline{K}/K)$ 是 $\overline{K}$ 在 K 上的 Galois 群, 则 G 是群 $\mathrm{Gal}(L/K)$ 的反向极限, 其中 L 跑遍 K 的所有有限 Galois 扩张, 于是 G 具有一个射影有限 (pro-finite) 群的结构. 而 G 在单位元 1 处的拓扑基由 G 的所有具有有限指标的正规子群给出. 一个 G 模被定义为一个 Abel 群 A, 其上具有一个连续的 G 作用, 即

$$G\times A\longrightarrow A$$

是连续的, 其中 G 的拓扑如上, 而 A 视为离散拓扑.

例如, $\overline{K}$ 以及 $\overline{K}^*$ 在 G 的自然作用下就成为一个 G 模 M, 也可以类似定义上同调群 $H^q(G,M)$, $q \geqslant 0$. 但此时要求上链是 $G^q \to M$ 的连续映射. 特别地, 当 $G = \mathrm{Gal}(\overline{K}/K)$ 时, 有

$$H^q(G,M) \cong \varinjlim H^q(\mathrm{Gal}(L/K),M),$$

其中 L/K 跑遍 K 的所有有限 Galois 扩张.

下面考虑 Brauer 群和 Galois 上同调之间的关系. 为此, 我们考虑具有下述性质的代数: 设 A 是 K 上的一个有限中心单代数, 而 L 是 K 的 Galois 扩张, 如果 $L \subset A$ 且 $\dim_L(A) = \dim_K(L)$, 则 A 称为一个交叉乘积.

我们知道, 每一个有限中心单代数 A 都通过 K 上一个有限 Galois 扩张分裂, 这等价于说 A 至少等价于一个 K 上的交叉乘积. 而研究交叉乘积的好处是它们具有简单的结构.

设 A 是一个交叉乘积, 则对每一个 $\sigma \in G = \mathrm{Gal}(L/K)$, 可以找到一个单位 $u_\sigma \in A$, 使得 $\{u_\sigma\}_{\sigma \in G}$ 是 A 的一个基 (将 A 视为 L 左向量空间) 并且有

$$u_\sigma x = \sigma(x) u_\sigma, \quad \forall x \in L, \forall \sigma \in G,$$
$$u_\sigma u_\tau = f(\sigma,\tau) u_{\sigma\tau}, \quad \forall \sigma,\tau \in G,$$

此处, $f:\ G \times G \to L^*$ 是一个 2 上闭链.

另一方面, 给定一个 2 上闭链 $f \in H^2(G,L^*)$, 其值在一个 n 次的 Galois 扩张 L/K 中, 则可以构造一个 n^2 维 K 向量空间

$$(L,G,f) = \bigoplus_{\sigma \in G} L u_\sigma.$$

而 (L,G,f) 中两个元素的乘法由下式给出:

$$\Big(\sum_{\sigma \in G} x_\sigma u_\sigma\Big)\Big(\sum_{\tau \in G} y_\tau u_\tau\Big) = \sum_{\sigma,\tau \in G} x_\sigma \sigma(y_\tau) f(\sigma,\tau) u_{\sigma\tau},$$

此处, $x_\sigma, y_\tau \in L$, 则 (L,G,f) 成为具有单位元 $f(1,1)^{-1}u_1$ 的有限中心单代数, 且它在 L 处分裂. (L,G,f) 称为 L 和 G 关于 f 的交叉乘积. 可以证明, 两个形如 (L,G,f) 和 (L,G,g) 的交叉乘积是同构的 K 代数当且仅当 f 和 g 只差一个 2 上边缘.

定理 18.5 我们有 $\mathrm{Br}(L/K) \cong H^2(G,L^*)$.

证明 设 f 和 g 是两个正规化的 2 上闭链 (即 $f(1,1) = g(1,1) = 1$). 考虑两个交叉乘积 (L,G,f) 和 (L,G,g), 则有

$$(L,G,f) \otimes (L,G,g) \sim (L,G,fg).$$

对于每一个 2 上闭链 g, 存在一个正规化 2 上闭链 $\widetilde{g}$, 它是上同调于 g 的 (即 $\widetilde{g}$ 与 g 属于同一个上同调类中), 从而导出映射

$$\alpha: \quad H^2(G, L^*) \longrightarrow \mathrm{Br}(L/K),\ [f] \longmapsto (L, G, f)$$

是一个良好定义的群同态.

首先说明 α 是满的: 这是因为 K 上的每一个在 L 处分裂的有限中心单代数 A 都等价于一个代数 B, 使得 $L \subset B$ 且 $\dim_L(B) = n$, 且存在一个 2 上闭链 f, 使得 $B \cong (L, G, f)$.

其次 α 是单的: 若 f 是一个 2 上闭链且 $(L, G, f) \sim K$, 由于 $\dim_K((L, G, f)) = n^2$, 故得出 $(L, G, f) \cong M_n(K)$. 下面考虑 L 和 G 关于平凡 2 上闭链 1 的交叉乘积, 有 $(L, G, 1) = \bigoplus_\sigma Lv_\sigma$, $v_\sigma v_\tau = v_{\sigma\tau}$ 且 $v_\sigma x = \sigma(x)v_\sigma$, $\forall \sigma, \tau \in G$, $x \in L$. 定义一个 K 代数同态如下:

$$\begin{aligned} \phi: \ (L, G, 1) \quad &\longrightarrow \quad \mathrm{End}_K(L), \\ \phi(xv_\sigma)(y) \quad &\longmapsto \quad x\sigma(y). \end{aligned}$$

由于 $(L, G, 1)$ 是单的, 可见 ϕ 是一个单射. 比较维数这意味着 ϕ 也是满射. 因此有 $(L, G, 1) \cong M_n(K) \cong (L, G, f)$. 这说明两个交叉乘积 $(L, G, 1)$ 和 (L, G, f) 是 K 代数同构的, 因此 f 和 1 只差一个 2 上边缘, 即 f 是上同调于 1 的, 从而 α 是单射. 定理证毕.

下面仅考虑 L/K 是 n 次循环 Galois 扩张的情形. 此时, 我们可以限定到下列简单形式的 2 上闭链:

设 $G = \mathrm{Gal}(L/K) = \langle\sigma\rangle$. 对于 $a \in K^*$, 定义映射

$$f_{\sigma,a}: \ G \times G \longrightarrow L^*, \quad f_{\sigma,a}(\sigma^i, \sigma^j) = \begin{cases} a, & \text{若 } i + j \geqslant n, \\ 1, & \text{若 } i + j < n, \end{cases}$$

显然, $f_{\sigma,a}$ 是一个正规化 2 上闭链. 设 (L, σ, a) 是交叉乘积 $(L, G, f_{\sigma,a})$ 并置 $u = u_\sigma$, 则显然有 $u^i = u_{\sigma^i}(i = 1, \cdots, n-1)$, 因此

$$(L, \sigma, a) = \bigoplus_{i=0}^{n-1} Lu^i,$$

而

$$u^n = a,\ ux = \sigma(x)u, \quad \forall x \in L,$$

于是得出每一个交叉乘积都同构于一个形如 (L, σ, a) 的代数. 事实上, 我们有

引理 18.2 设 f 是一个正规化 2 上闭链, 则

$$(L,G,f)\cong(L,\sigma,a),$$

其中 $a=\prod_{m=0}^{n-1}f(\sigma^m,\sigma)\in K^*$.

证明 我们有 $(L,G,f)=\bigoplus_{i=0}^{n-1}Lv_{\sigma^i}$, $v_1=1$, $v_{\sigma^i}x=\sigma^i(x)v_{\sigma^i}$, $\forall x\in L$. 更进一步, 有 $v_{\sigma^i}v_{\sigma^j}=f(\sigma^i,\sigma^j)v_{\sigma^{i+j}}$, $0\leqslant i,j\leqslant n-1$. 现在

$$\begin{aligned}v_\sigma^2&=v_\sigma v_\sigma=f(\sigma,\sigma)v_{\sigma^2},\\ v_\sigma^3&=f(\sigma,\sigma)v_{\sigma^2}v_\sigma=f(\sigma,\sigma)f(\sigma^2,\sigma)v_{\sigma^3}.\end{aligned}$$

一般地, 有

$$v_\sigma^i=\Big(\prod_{j=1}^{i-1}f(\sigma^j,\sigma)\Big)v_{\sigma^i},\quad i=2,\cdots,n-1.$$

考虑 v_σ^n, 有 $v_\sigma^n=av_{\sigma^n}=a$. 因此 $(L,G,f)=\bigoplus_{i=0}^{n-1}Lv_\sigma^i$ (因为 $\prod_{j=0}^{i-1}f(\sigma^j,\sigma)\in L^*$, $2\leqslant i\leqslant n-1$), 我们也有 $v_\sigma^n=a$ 且 $v_\sigma x=\sigma(x)v_\sigma$, $\forall x\in L$. 因此 $(L,G,f)\cong(L,\sigma,a)$. 由于 $a=v_\sigma^n$ 位于 (L,G,f) 的中心之内, 故有 $a\in K$. 引理证毕.

下面的定理表明相对 Brauer 群 $\mathrm{Br}(L/K)$ 可以借助基域 K 而得到完全的描述:

定理 18.6 设 L/K 是 n 次的循环Galois扩张, $G=\mathrm{Gal}(L/K)=\langle\sigma\rangle$, 则映射 ϕ: $a\mapsto(L,\sigma,a)$ 诱导出一个同构

$$K^*/N_{L/K}(L^*)\xrightarrow{\ \sim\ }\mathrm{Br}(L/K).$$

证明 (L,σ,a) 在 L 处分裂, 因此 $[(L,\sigma,a)]\in\mathrm{Br}(L/K)$. 因为 $f_{\sigma,a}f_{\sigma,b}=f_{\sigma,ab}$, 我们也有 $\phi(a)\phi(b)=\phi(ab)$. 设 A 是在 L 处分裂的一个有限中心单代数, 则存在正规化 2 上闭链 f, 使得 $A\sim(L,G,f)$. 因而存在 $a\in K^*$, 使得 $(L,G,f)\sim(L,\sigma,a)$ (引理 18.2). 从而 $A\sim(L,\sigma,a)$, 因此 ϕ 是满的.

现在只需再证明

$$(L,\sigma,a)\cong(L,\sigma,1)\iff a\in N_{L/K}(L^*).$$

设 $(L,\sigma,a)=\bigoplus_i Lu^i$, $(L,\sigma,1)=\bigoplus_i Lv^i$. 假设 $a=N_{L/K}(y)$, $y\in L^*$, 则考虑 $\widetilde{u}=y^{-1}u$, 知

$$\begin{aligned}\widetilde{u}^n&=y^{-1}uy^{-1}u\cdots y^{-1}u=y^{-1}\sigma(y^{-1})u^2y^{-1}\cdots y^{-1}u=\cdots\\ &=\Big(\prod_{i=0}^{n-1}\sigma^i(y^{-1})\Big)u^n=N_{L/K}(y^{-1})a=a^{-1}a=1.\end{aligned}$$

更进一步, 有

$$\widetilde{u}x = y^{-1}ux = y^{-1}\sigma(x)u = \sigma(x)y^{-1}u = \sigma(x)\widetilde{u},$$

因此 $(L,\sigma,a) \cong (L,\sigma,1)$.

反之, 考虑一个 K 代数同构 ψ: $(L,\sigma,a) \simeq (L,\sigma,1)$, 应用 Skolem-Noether 定理 18.2, 存在 α, 使得

$$x \times 1 = \alpha\psi(x)\alpha^{-1}, \quad \forall x \in L.$$

考虑 $w = \alpha\phi(u)\alpha^{-1}$, 则得出 $w^n = a$, $wxw^{-1} = \sigma(x)$ 且 $wx = \sigma(x)w$, $\forall x \in L$. 设 v 是用来定义平凡代数 $(L,\sigma,1)$ 的, 令 $y = wv^{n-1}$, 我们获得

$$yx = wv^{n-1}x = w\sigma^{n-1}(x)v^{n-1} = \sigma(\sigma^{n-1}(x))wv^{n-1} = xy,$$

从而 $y \in Z_{(L,\sigma,1)}(L) = L$. 更进一步, 有

$$\begin{aligned} a = w^n &= yvyv\cdots yv = y\sigma(y)v^2yv\cdots yv = \cdots \\ &= y\sigma(y)\sigma^2(y)\cdots\sigma^{n-1}(y)v^n = N_{L/K}(y)v^n = N_{L/K}(y), \end{aligned}$$

此处用到了事实 $v^n = 1$, 这是由 v 和 $(L,\sigma,1)$ 的定义显见的, 由此可见 $a = N_{L/K}(y)$. 于是定理得证.

§18.2　Brauer 群及有限域中的离散对数问题

我们在本节考虑局部域和整体域的 Brauer 群, 并将它们与有限域上的离散对数问题联系起来.

设 K 是一个局部域, 即存在 K 上的一个离散赋值 v, 使得 K 关于 v 是完备的, 并且 K 关于 v 的剩余类域 k 是一个有限域. 若 D 是 K 上的一个有限维斜域, 则离散赋值 v 可惟一扩充到 D 的一个赋值 v_D. 这个赋值可借助 v 给出:

$$v_D(x) = \frac{1}{n}v_K(N_{D/K}(x)).$$

此处 n 是 D 在 K 上的维数, 而一个元素 $d \in D/K$ 的范数 $N_{D/K}(d)$ 定义作 K 线性映射 $x \to dx$ 的行列式. 令 R_D 是 D 的赋值环, $\wp$ 是其最大理想, 我们有 $k_\wp = R_D/\wp$. 由 v_D 的定义, 存在 $n = [D:K]$ 的一个因子 e, 使得 $v_D(D^*) = \frac{1}{e}\mathbb{Z}$, e 称为 D 的分歧指标. 若一个有限扩张 L/K 的分歧指标等于 1, 则 L/K 称为一个非分歧的扩张, 而对应的剩余类域的扩张是可分的. 若 L/K 是任意一个 n 次的局部扩张, 则伴随的剩余类域扩张是一个 f 次的有限扩张 (f 称为剩余类次数). 于是我们有基本的关系式

$$n = ef.$$

固定 K 的一个代数闭包 $\overline{K}$, 对于每一个自然数 n, 在 $\overline{K}$ 中恰存在一个 n 次非分歧扩张 K_n/K, 使得 K_n/K 是循环 Galois 扩张. 令 $q=|k|$, 则 Galois 群 $\mathrm{Gal}(K_n/K)$ 具有一个典范生成元 Frobenius 自同构 $\sigma_\wp$, 它诱导出剩余类域的 Forbenius 自同构: $x\mapsto x^q$.

在 §18.1 中, 我们说过只要研究相对 Brauer 群 $\mathrm{Br}(L/K)$ 即可, 此处 L/K 是有限 Galois 扩张. 下面首先考虑 L/K 是非分歧的情形, 然后证明 $\mathrm{Br}(K)$ 中每个元素都在 K 的某个非分歧扩张处是分裂的.

由定理 18.6, 当 L/K 是循环 Galois 扩张时, $\mathrm{Br}(L/K)$ 的研究等价于范映射 $N_{L/K}$ 的研究.

引理 18.3 设 K 为局部域, L/K 是一个有限次循环非分歧扩张, 则每一个元素 $u\in U_K$ 都是 L 的一个单位的范数, 因此, 范映射 $N_{L/K}:U_L\to U_K$ 是满射, 此处 U_K,U_L 分别是 K,L 的单位群.

证明 记 $U_L^m=1+\wp_L^m$, $U_K^m=1+\wp_K^m$, 引进 U_L 和 U_K 的滤子如下:

$$\cdots U_L^{m+1}\subset U_L^m\subset\cdots\subset U_L^2\subset U_L^1\subset U_L$$

和

$$\cdots U_K^{m+1}\subset U_K^m\subset\cdots\subset U_K^2\subset U_K^1\subset U_K.$$

在这些滤子上检验范映射: 令 $x=1+y$, $y\in\wp_L^n$, 则 $\sigma(x)=1+\sigma(y)$, $\forall\sigma\in G$, 且有 $\sigma(y)\in\wp_L^n$, 因此

$$N_{L/K}(x)=\prod_{\sigma\in G}(1+\sigma(y))\equiv 1+\sum_{\sigma\in G}\sigma(y)\pmod{\wp_L^{2n}}. \tag{18.1}$$

由于 L/K 是非分歧的, 故有 $\wp_L^n\cap K=\wp_K^n$, 因此 $N_{L/K}(x)\equiv 1\pmod{\wp_K^n}$. 过渡到商群, 范映射诱导出映射

$$N_n:\ U_L^n/U_L^{n+1}\longrightarrow U_K^n/U_K^{n+1}.$$

现在检验每一个 N_n. 首先注意到 U_L/U_L^1 可以等同于剩余类域 l 的乘法群, 而对 $n>1$, 可以将 U_L^n/U_L^{n+1} 等同于 $\wp_L^n/\wp_L^{n+1}$, 而后者是 l 上的一维向量空间 Ω_L^n. 由于 L/K 非分歧, 故可以将 Ω_L^n 等同于 $\Omega_K^n\bigotimes_K l$. 映射 N_i 可描述如下: 对 $i=0$, 映射 $N_0:\ l^*\to k^*$ 正好是剩余类域扩张 l/k 的范映射; 而由于 (18.1) 式, 每个 $N_i: l\bigotimes_K\Omega_K^n\ (i\geqslant 1)$ 正好是映射 $1\otimes Tr_{L/K}$. 由于在任何可分扩张中, 迹映射是满射, 又由于 (18.1) 式, 故显然有

$$N_n:\ U_L^n/U_L^{n+1}\longrightarrow U_K^n/U_K^{n+1}$$

是满的. 现在, 应用下述事实:

设有双射 $U_L \cong \varinjlim U_L/U_L^n$, $U_K \cong \varinjlim U_K/U_K^n$, 则映射

$$N_n: \ U_L^n/U_L^{n+1} \longrightarrow U_K^n/U_K^{n+1}$$

是满的意味着 $N: \ U_L \to U_K$ 是满的.

由于前面已说明了 N_n 是满的. 于是上述事实就表明 $N: \ U_L \to U_K$ 是满的, 引理证毕.

定理 18.7 设 K_n/K 是 K 的次数为 n 的惟一非分歧扩张, 而 σ 是Frobenius自同构, 则映射 (其中 π 是 K 的一致化元)

$$\theta: \ \mathbb{Z} \longrightarrow \mathrm{Br}(K_n/K), \quad k \longmapsto [(K_n/K, \sigma, \pi^k)]$$

诱导出一个同构

$$\theta_n: \ \mathbb{Z}/n\mathbb{Z} \cong \mathrm{Br}(K_n/K).$$

证明 易知 $k \mapsto [(K_n/K, \sigma, \pi^k)]$ 定义了一个群同态, 它诱导出一个映射 $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Br}(K_n/K)$. 下证这个诱导出的映射是满的：由于 $\mathrm{Br}(K_n/K)$ 中一个元素 A 具有形式 $(K_n/K, \sigma, a)$, $a \in K^*$. 令 $a = u\pi^k$, 其中 u 为单位, 则

$$A \sim (K_n/K, \sigma, u) \bigotimes_K (K_n/K, \sigma, \pi^k) \sim (K_n/K, \sigma, \pi^k),$$

其中用到了下述事实：K 中每一个单位都是非分歧扩张 K_n/K 的一个范数, 因而属于 u 的代数 $(K_n/K, \sigma, u)$ 是平凡的 (定理 18.6).

可见, $\mathrm{Br}(K_n/K)$ 中每个元素都是映射 $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Br}(K_n/K)$ 的像, 从而该映射是满的. 另一方面, 如果我们有

$$1 = [(K_n/K, \sigma, \pi^k)] \in \mathrm{Br}(K_n/K),$$

则由定理 18.6, 有 $\pi^k = N_{K_n/K}(y), y \in K_n^*$, 从而

$$n v_{K_n}(y) = v_k(N_{K_n/K}(y)) = v_K(\pi^k) = k.$$

可见 $k \equiv 0 \pmod{n}$. $\mathbb{Z}/n\mathbb{Z} \to \mathrm{Br}(K_n/K)$ 是单射, 因此 θ_n 是一个同构. 定理证毕.

定理 18.8 设 K 是一个局部域, 则有同构

$$\theta: \ \mathbb{Q}/\mathbb{Z} \cong \mathrm{Br}(K), \quad \theta\left(\frac{k}{n} \pmod{\mathbb{Z}}\right) = [(K_n/K, \sigma_n, \pi^k)],$$

此处, $n \in \mathbb{N}$, $0 \leqslant k \leqslant n$, σ_n 记 K_n/K 的Frobenius元.

证明 显然 $\mathbb{Q}/\mathbb{Z}=\bigcup_{n\in\mathbb{N}}\frac{1}{n}\mathbb{Z}/\mathbb{Z}$, 另一方面, 又有 $\mathrm{Br}(K)=\bigcup_{n\in\mathbb{N}}\mathrm{Br}(K_n/K)$. 而对于 Brauer 群, 由定理 18.7, 我们有同构 $\theta_n:\ \mathbb{Z}/n\mathbb{Z}\cong\mathrm{Br}(K_n/K)$, 但是 $\frac{1}{n}\mathbb{Z}/\mathbb{Z}\cong\mathbb{Z}/n\mathbb{Z}$, 因此 $\frac{1}{n}\mathbb{Z}/n\mathbb{Z}\cong\mathrm{Br}(K_n/K)$. 而对于给定的 $m,n\in\mathbb{N}$, 易知下面的图表是交换的:

$$\begin{array}{ccc}\frac{1}{n}\mathbb{Z}/\mathbb{Z} & \longrightarrow & \frac{1}{mn}\mathbb{Z}/\mathbb{Z}\\ \downarrow & & \downarrow\\ \mathrm{Br}(K_n/K) & \longrightarrow & \mathrm{Br}(K_{mn}/K)\end{array}$$

因此, 得到一个同构 $\mathbb{Q}/\mathbb{Z}\cong\mathrm{Br}(K)$. 定理证毕.

定义 18.4 *定理18.8中映射 θ 的逆映射 θ^{-1} 称为不变量映射, 记为 inv. 即*

$$\mathrm{inv}:\ \mathrm{Br}(K)\longrightarrow\mathbb{Q}/\mathbb{Z},\quad [A]=[(K_n/K,\sigma_n,\pi^k)]\longmapsto\mathrm{inv}(A)=\frac{k}{n}\pmod{\mathbb{Z}}.$$

设 K 是一个数域, 即 $\mathbb{Q}$ 的一个有限代数扩张. 而 S 记 K 的位 $\wp$ 的代表元的集合. 除了非阿位 $\wp$ 外 (此时 $K_\wp$ 是局部域), 我们也要考虑阿基米德素除子 $\wp$(此时 $K_\wp$ 是 $\mathbb{C}$ 和 $\mathbb{R}$). 对于局部 Brauer 群, 有

(1) 若 $\wp$ 是非阿氏位, 则 $K_\wp$ 为局部域, 因而定理 18.8 告诉我们有

$$\mathrm{Br}(K_\wp)\cong\mathbb{Q}/\mathbb{Z};$$

(2) 若 $\wp$ 是一个实位, 即 $K_\wp\cong\mathbb{R}$, 则定理 18.3(iii) 告诉我们有

$$\mathrm{Br}(K_\wp)\cong\mathbb{Z}/2\mathbb{Z}\cong\frac{1}{2}\mathbb{Z}/\mathbb{Z}\subset\mathbb{Q}/\mathbb{Z};$$

(3) 若 $\wp$ 是一个复位, 即 $K_\wp\cong\mathbb{C}$, 则定理 18.3(ii) 告诉我们有 $\mathrm{Br}(K_\wp)=1$.

对于每一个位 $\wp$, 我们有嵌入 $K\mapsto K_\wp$, 从而诱导出一个群同态

$$\alpha:\ \mathrm{Br}(K)\longrightarrow\bigoplus_{\wp}\mathrm{Br}(K_\wp).$$

而关于整体域的 Brauer 群, 最重要的事实就是整体 Brauer 群的元素由其在上述同态下的像完全描述. 即

定理 18.9 (Hasse-Brauer-Noether) *存在一个正合序列如下:*

$$0\longrightarrow\mathrm{Br}(K)\stackrel{\alpha}{\longrightarrow}\bigoplus_{\wp\in S}\mathrm{Br}(K_\wp)\longrightarrow\mathbb{Q}/\mathbb{Z}\longrightarrow 0,\tag{18.2}$$

此处最后的映射定义为

$$(A_\wp)_{\wp\in S}\mapsto\sum_{\wp\in S}\mathrm{inv}(A_\wp).$$

下面讨论有限域中的离散对数问题与 Brauer 群之间的关系. 令 $k=\mathbb{F}_q$ 是一个有限域, l 为一正整数, $l|q-1$, 即 k 含有 l 次单位根. 于是我们考虑 l 次单位根群的离散对数问题: 给定两个非平凡的 l 次单位根 ζ_0 和 $\zeta_1\in\langle\zeta_0\rangle$, 决定 $n \pmod l$, 使得 $\zeta_1=\zeta_0^n$. 设 K 是一个局部域, 其剩余类域 $k=\mathbb{F}_q$, 而 L/K 是一个次数 l 的分歧循环 Galois 扩张, $l\neq \mathrm{char}(k)$, $\mathrm{Gal}(L/K)=\langle\sigma\rangle$.

引理 18.4 设 K 是 $\mathbb{Q}_p$ 的有限扩张, 其剩余类域为 k, 设 L/K 是一个素数次 $l(\neq p)$ 的分歧扩张 ($l\neq p$ 意味着 K^* 包含 l 次单位根群 μ_l), 则有

$$\mathrm{Br}(L/K)\cong k^*/(k^*)^l\cong\mu_l(k).$$

证明 由定理 18.6, 有 $\mathrm{Br}(L/K)\cong K^*/N_{L/K}(L^*)$, 因此我们需要检验分歧扩张 L/K 的范映射.

K 中每一个元素均可表示为 $u\cdot\pi^i$, $u\in U_K$, $i\in\mathbb{Z}$. 由于 L/K 是分歧的, π 是一个范数, 因此我们只要考虑 L 的单位群 U_L. 考虑滤子

$$\cdots U_L^i\subset U_L^{i-1}\subset\cdots\subset U_L^1\subset U_L$$

和

$$\cdots U_K^i\subset U_K^{i-1}\subset\cdots\subset U_K^1\subset U_K,$$

此处, 对 $i\geqslant 1$, 有 $U_L^i=1+\wp_L^i$, $U_K^i=1+\wp_K^i$.

由于 L/K 是 tamely 分歧的 (条件 $l\neq p$), 所有的商群 U_K^i/U_K^{i+1} $(i\geqslant 1)$ 均是范映射的像. 只有情形 $U_L/U_L^1\to U_K/U_K^1$ 需要验证. 我们有 $U_L/U_L^1\cong\mathscr{F}^*$, $U_K/U_K^*\cong k^*$, 其中 $\mathscr{F}$ 记 L 的剩余类域. 由于 L/K 是分歧的, 故有 $\mathscr{F}=k$. 因此 U_L/U_L^1 在范映射下的像是 $(k^*)^l$, 于是有

$$K^*/N_{L/K}(L^*)\cong k^*/k^{*l}.$$

但是映射

$$k^*/k^{*l}\longrightarrow\mu_l\quad x\pmod{k^{*l}}\longmapsto x^{\frac{q-1}{l}}$$

给出一个同构, 因此

$$\mathrm{Br}(L/K)\cong k^*/k^{*l}\cong\mu_l.$$

这就完成了证明.

定理 18.6 和引理 18.4 给出了一个同构 $\mu_l(k)\cong\mathrm{Br}(L/K)$, $\zeta\mapsto(L,\sigma,\zeta)\in\mathrm{Br}(L/K)$. 现在就可以将 $\mu_l\subset\mathbb{F}_q^*$ 中的离散对数问题与 $\mathrm{Br}(L/K)$ 联系如下: 给定两个 l 次单位根 ζ_0 和 $\zeta_1=\zeta_0^n$, 选取一个扩张 $K/\mathbb{Q}_p$, 使得 K 的剩余类域为 $k=\mathbb{F}_q$. 同时选取次数为 l 的分歧 Galois 扩张 L/K. 令 $\mathrm{Gal}(L/K)=\langle\sigma\rangle$, 于是可以构造

循环代数 $A_0 = (L/K, \sigma, \zeta_0)$ 和 $A_1 = (L/K, \sigma, \zeta_1)$. 如果我们能够计算 $\mathrm{inv}(A_0)$ 和 $\mathrm{inv}(A_1)(= n\mathrm{inv}(A_0))$, 则离散对数 n 就可以通过计算

$$\mathrm{inv}(A_1)/\mathrm{inv}(A_0) \pmod l$$

而得到.

因此, μ_l 中的离散对数的计算就转化为下述计算问题: 给定一个循环代数 $A = (L/K, \sigma, \zeta)$, 其中 L/K 是素数次数 l 的一个 tamely 分歧扩张, 计算 $[A] \in \mathrm{Br}(K)$ 的不变量, 即计算 $\mathrm{inv}(A) = \theta^{-1}([A])$.

§18.3 不变量映射的局部计算

在本节中, 我们关注局部域上不变量映射 inv 的清晰计算方法. 我们的办法是利用 Galois 上同调.

设 K 是一个局部域, 它关于离散赋值 $\wp$ 是完备的. $k_\wp$ 记 K 关于 $\wp$ 的剩余类域, 设 $k_\wp = \mathbb{F}_q$. 下面假定 $l|q-1$, 因而 K 含有 l 次单位根群. 设 L/K 是一个非分歧扩张, 次数为 l(素数). 由于我们假定 K 含有 l 次单位根群, 由 Kummer 理论知存在 $\alpha \in K^*/K^{*l}$, 使得 $L = K(\alpha^{1/l})$. 域扩张 L/K 是循环 Galois 扩张, 设 $\mathrm{Gal}(L/K) = \langle\sigma\rangle$.

考虑 $\mathrm{Br}(K)$ 中一个 l 阶元素, 它由下述 2 上闭链给出:

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \beta, & i+j \geqslant l, \\ 1, & i+j < l. \end{cases}$$

令 U_L 和 U_K 分别是 L 和 K 的单位群, 正如引理 18.3 所述, U_K 中每一个元素都是 U_L 中一个元素的范数. 设 π 是一个素元, 则可以假定 β 具有形式 $\beta = \pi^n$. 于是有

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \pi^n, & i+j \geqslant l, \\ 1, & i+j < l. \end{cases}$$

若 σ 是 Frobenius 元 $\sigma_\wp$, 则不变量映射能够立即计算出来 (因为由定义, 有 $\mathrm{inv}(\phi(\sigma_\wp^i, \sigma_\wp^j)) \equiv n \pmod l$).

假设 $\sigma^k = \sigma_\wp$, 则有

$$(L, \sigma, \pi^n) \cong (L, \sigma^k, \pi^{nk}) \cong (L, \sigma_\wp, \pi^{nk}).$$

因此, $\mathrm{inv}(\phi(\sigma^i, \sigma^j)) \equiv nk \pmod l$. 在此情形下, 不变量映射的计算就转化为描述 $\mathrm{Gal}(L/K)$ 的一个生成元和 L/K 的 Frobenius 元 $\sigma_\wp$ 之间的关系. 即在 $\mathrm{Gal}(L/K)$

中解离散对数问题. 由于我们面对的是 Kummer 扩张情形, 这个问题可如下进行: 回忆 σ 作用在 $\gamma = \alpha^{1/l}$ 上, $\sigma(\gamma) = \zeta_l\gamma$, ζ_l 是一个本原 l 次单位根. 设 $\overline{x}$ 是一个元素 $x \in K$ 在剩余类域 $k_\wp = \mathbb{F}_q$ 中的约化. Frobenius 自同构作用在扩张 $\mathscr{F}_\wp/k_\wp$ 上: $\sigma_\wp(\overline{x}) = \overline{x}^q$, 因此 Frobenius 在 $\overline{\gamma}$ 上的作用由下式给出:

$$\sigma_\wp(\overline{\gamma})/\overline{\gamma} = \overline{\gamma}^q/\overline{\gamma} = \overline{\alpha}^{q/l}/\overline{\alpha}^{1/l} = \overline{\alpha}^{(q-1)/l}. \tag{18.3}$$

为了描述 σ 作为 Frobenius 的幂次 $(\sigma = \sigma_\wp^k)$, 我们必须解 $\mathbb{F}_q$ 中离散对数: $\left(\overline{\alpha}^{(q-1)/l}\right)^k = \overline{\zeta_l}$.

下面, 设 L/K 是一个素数次数 l 的 tamely 分歧扩张. $l \neq \mathrm{char}(k_\wp)$ 且 $\zeta_l \in K^*$. 同时假定 $\zeta_{l^2} \notin K$. 设 $\mathrm{Gal}(L/K) = \langle\sigma\rangle$ 是 l 阶循环群, 考虑 $\mathrm{Br}(K)$ 中一个 l 阶元素, 它由下述 2 上闭链给出:

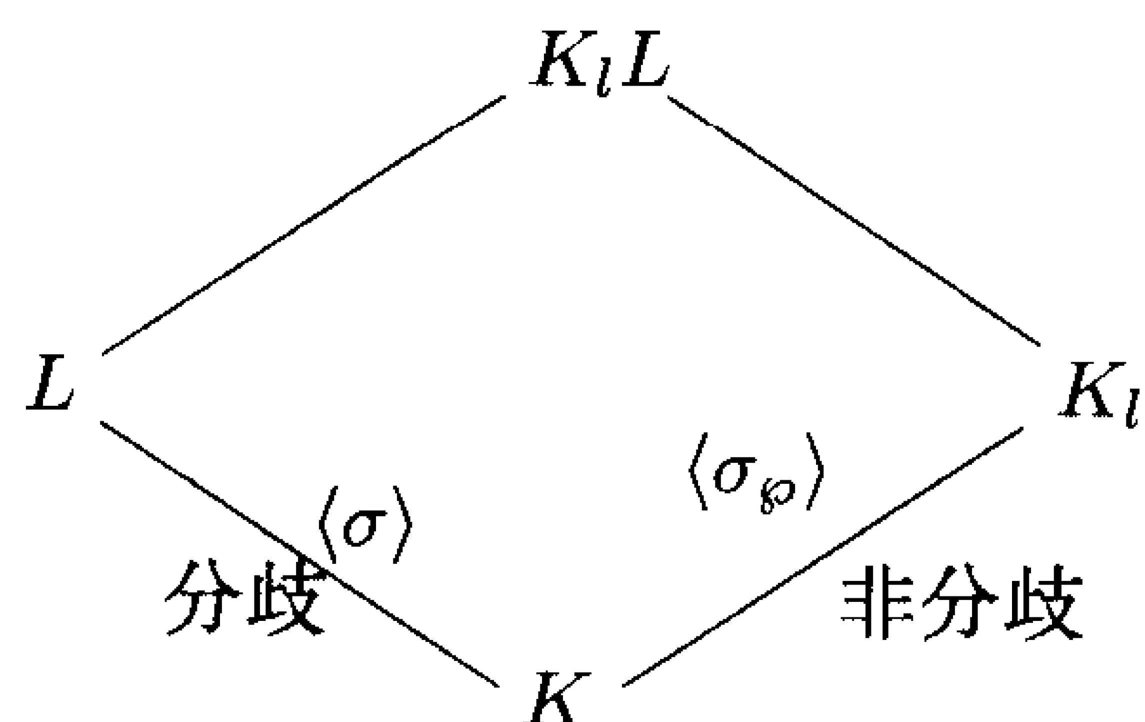
$$\phi(\sigma^i, \sigma^j) = \begin{cases} \beta, & i+j \geqslant l, \\ 1, & i+j < l, \end{cases} \qquad \beta \in K^*/N_{L/K}(L^*).$$

由引理 18.4, 有

$$K^*/N_{L/K}(L^*) = k_\wp^*/{k_\wp^*}^l \cong \langle\zeta_l\rangle.$$

于是可以假定 $\beta \in \langle\zeta_l\rangle$.

为了计算 ϕ 所对应的代数的不变量, 考虑下述情形: 设 L/K 是 l 次循环 tamely 分歧扩张, 而 K_l/K 是 l 次非分歧扩张, $\mathrm{Gal}(K_l/K) = \langle\sigma_\wp\rangle$, $\sigma_\wp$ 是 Frobenius 自同构. 我们有下述图表:



于是有 Galois 上同调图表如下:

$$\begin{array}{ccc} & H^2(K_lL/K, (K_lL)^*) & \\ \nearrow^{\mathrm{infl}_L^{K_lL}} & & \nwarrow^{\mathrm{infl}_{K_l}^{K_lL}} \\ H^2(L/K, L^*) & & H^2(K_l/K, K_l^*) \end{array}$$

我们的任务可描述如下：必须找到一个上闭链 $\psi \in H^2(K_l/K,(K_l)^*)$，使得 $\widehat{\psi} = \mathrm{infl}_{K_l}^{K_lL}(\psi)$ 和 $\widehat{\phi} = \mathrm{infl}_{L}^{K_lL}(\phi)$ 仅差一个上边缘.

下面清晰地描述两个上闭链 ϕ 和 ψ 的 inflations $\widehat{\phi}$ 和 $\widehat{\psi}$：令 $\mathrm{Gal}(L/K) = \langle\sigma\rangle$，$\mathrm{Gal}(K_l/K) = \langle\sigma_\wp\rangle$，于是 $\mathrm{Gal}(LK_l) = \langle\sigma, \sigma_\wp\rangle$，则有

$$\widehat{\phi}(\sigma^i\sigma_\wp^j, \sigma^r\sigma_\wp^s) = \phi(\sigma^i, \sigma^r), \quad 1 \leqslant i,j,r,s \leqslant l,$$

且

$$\widehat{\psi}(\sigma^i\sigma_\wp^j, \sigma^r\sigma_\wp^s) = \psi(\sigma_\wp^j, \sigma_\wp^s), \quad 1 \leqslant i,j,r,s \leqslant l.$$

$\widehat{\phi}$ 与 $\widehat{\psi}$ 是上同调的当且仅当存在一个映射 θ：$\mathrm{Gal}(K_lL/K) \to (K_lL)^*$，使得

$$\widehat{\phi}(z_1, z_2) = \widehat{\psi}(z_1, z_2)\theta(z_2)\theta(z_1z_2)^{-1}\theta(z_1)^{z_2}$$

对所有 $z_1, z_2 \in \mathrm{Gal}(LK_l/K)$ 成立. 函数 θ 由它在 σ 和 $\sigma_\wp$ 处的值所决定.

引理 18.5 函数 θ 具有下述性质：

(1) $\theta(1) = 1$;

(2) $\beta = N_{LK_l/K_l}(\theta(\sigma))$;

(3) $\pi^{-n} = N_{LK_l/L}(\theta(\sigma_\wp))$;

(4) $\theta(\sigma\sigma_\wp) = \theta(\sigma_\wp)\theta(\sigma)^{\sigma_\wp} = \theta(\sigma)\theta(\sigma_\wp)^{\sigma}$.

证明 (1) 是显然的. 由 θ 的定义，有

$$\theta(\sigma)\theta(\sigma^{i+1})^{-1}\theta(\sigma^i)^\sigma = \widehat{\phi}(\sigma^i, \sigma)\widehat{\psi}(\sigma^i, \sigma)^{-1}. \tag{18.4}$$

由于 $\widehat{\phi}(\sigma^i, \sigma) = \phi(\sigma^i, \sigma) = 1$, $i < l-1$, $\widehat{\psi}(\sigma^i, \sigma) = \psi(1,1) = 1$，于是由 (18.4) 式有

$$\theta(\sigma^{i+1}) = \theta(\sigma)\theta(\sigma^i)^\sigma. \tag{18.5}$$

从而对 $i < l-1$，有

$$\theta(\sigma^{i+1}) = \theta(\sigma)\theta(\sigma)^\sigma \cdots \theta(\sigma)^{\sigma^i}. \tag{18.6}$$

对 $i = l-1$，由 (18.4) 式及 $\theta(\sigma^l) = \theta(1) = 1$，有

$$\begin{aligned}\theta(\sigma)\theta(\sigma^l)^{-1}\theta(\sigma^{l-1})^\sigma = \theta(\sigma)\theta(\sigma^{l-1})^\sigma &= \widehat{\phi}(\sigma^{l-1}, \sigma)\widehat{\psi}(\sigma^{l-1}, \sigma)^{-1} \\ &= \phi(\sigma^{l-1}, \sigma)\psi(1,1) = \beta.\end{aligned} \tag{18.7}$$

由 (18.6) 式，有

$$\beta = \theta(\sigma)\theta(\sigma)^\sigma \cdots \theta(\sigma)^{\sigma^{l-1}}. \tag{18.8}$$

因为 L/K 是循环 Galois 扩张，且 $\mathrm{Gal}(L/K) = \langle\sigma\rangle$，因此

$$\beta = \prod_{i=0}^{l-1} \theta(\sigma)^{\sigma^i} = N_{L/K}(\theta(\sigma)). \tag{18.9}$$

这就证明了 (2).

(3) 与 (2) 类似, 考虑 $\theta(\sigma_\wp)$, 有

$$\theta(\sigma_\wp^{i+1}) = \theta(\sigma_\wp)\theta(\sigma_\wp)^{\sigma_\wp} \cdots \theta(\sigma_\wp)^{\sigma_\wp^i}, \ i < l-1. \tag{18.10}$$

由于 $\widehat{\phi}(\sigma_\wp^{l-1}, \sigma_\wp) = \phi(1,1)$, $\widehat{\psi}(\sigma_\wp^{l-1}, \sigma_\wp) = \psi(\sigma_\wp^{l-1}, \sigma_\wp) = \pi^n$, 故有

$$\pi^{-n} = \prod_{i=0}^{l-1} \theta(\sigma_\wp)^{\sigma_\wp^i} = N_{K_l/K}(\theta(\sigma_\wp)), \tag{18.11}$$

此处用到了事实: K_l/K 是循环 Galois 的且 $\mathrm{Gal}(K_l/K) = \langle\sigma_\wp\rangle$.

(4) 考虑 $\theta(\sigma\sigma_\wp)$, 有

$$\widehat{\phi}(\sigma, \sigma_\wp) = \phi(\sigma, 1) = 1 = \phi(1, \sigma) = \widehat{\phi}(\sigma_\wp, \sigma),$$

$$\widehat{\psi}(\sigma, \sigma_\wp) = \psi(1, \sigma_\wp) = 1 = \psi(\sigma_\wp, 1) = \widehat{\psi}(\sigma_\wp, \sigma).$$

应用 θ 的定义和 (18.4) 式, 有

$$\theta(\sigma_\wp)\theta(\sigma\sigma_\wp)^{-1}\theta(\sigma)^{\sigma_\wp} = \theta(\sigma)\theta(\sigma\sigma_\wp)^{-1}\theta(\sigma_\wp)^{\sigma},$$

因此

$$\theta(\sigma_\wp)\theta(\sigma)^{\sigma_\wp} = \theta(\sigma)\theta(\sigma_\wp)^{\sigma}.$$

这就完成了引理的证明.

定理 18.10　设 K 为局部域, $\zeta_l \in K$, $\zeta_{l^2} \notin K$. 设 π 是 K 的一个元素, 使得 $v(\pi) = 1$. 设 K_l/K 是次数 l 的非分歧扩张, 其Galois群为 $\mathrm{Gal}(K_l/K)$, 而 $\sigma_\wp$ 是其Frobenius自同构. 将 $K_l = K(\alpha^{1/l})$ 视为一个Kummer扩张, 固定 l 次单位根 ζ 如下:

$$\sigma_\wp(\alpha^{1/l}) = \zeta\alpha^{1/l}.$$

设 $L = K(\pi^{1/l})/K$ 是次数 l 的循环分歧扩张 ($l \neq \mathrm{char}(k_\wp)$) 且 $\mathrm{Gal}(L/K) = \langle\sigma\rangle$, 此处 σ 由 $\sigma(\pi^{1/l}) = \zeta\pi^{1/l}$ 所定义. 又设 $\phi \in H^2(\langle\sigma\rangle, L^*)$ 如下给出:

$$\phi(\sigma^i, \sigma^j) = \begin{cases} \zeta^m, & i+j \geqslant l, \\ 1, & i+j < l. \end{cases}$$

而 $\psi \in H^2(K_l/K, K_l^*) = H^2(\langle\sigma_\wp\rangle, K_l^*)$ 由下式给出:

$$\psi(\sigma_\wp^i, \sigma_\wp^j) = \begin{cases} \pi^n, & i+j \geqslant l, \\ 1, & i+j < l, \end{cases}$$

则当 $n \equiv -tm \pmod l$ 时, ϕ 和 ψ 在 $H^2(\mathrm{Gal}(LK_l/L), (LK_l)^*)$ 中是上同调的, 其中 $t \equiv \frac{q-1}{l} \pmod l$.

推论 18.1 $\mathrm{Br}(K)$ 中由 ϕ 给出的元素具有不变量 $-tm \pmod{l}$.

证明 首先计算 $\theta(\sigma)$ 和 $\theta(\sigma_\wp)$. 引理 18.5 (4) 给出了这些元素和 σ 及 $\sigma_\wp$ 在其作用之间的一个关系, 不变量可以由这个关系式计算出来. 引理 18.5 (1) 表明 $\beta = N_{LK_l/K_l}(\theta(\sigma))$, 由于 $\zeta_l \in K$ 且 $\zeta_{l^2} \notin K$, K 上的次数 l 的一个非分歧扩张由 $\zeta^{1/l}$ 所定义. 由于这个扩张是惟一决定的, 故有 $\zeta^{1/l} \in L$. 因此, 由 $\beta = \zeta^m$, 有 $\beta = ((\zeta^m)^{1/l})^l = N_{LK_l/K_l}((\zeta^m)^{1/l})$, 从而

$$N_{LK_l/K_l}\Big(\frac{\theta(\sigma)}{(\zeta^m)^{1/l}}\Big) = 1.$$

Hilbert 定理 90 意味着存在 $x_1 \in (LK_l)^*$, 使得

$$\theta(\sigma) = (\zeta^m)^{1/l} x_1^{\sigma-1}, \quad x_1 \in (LK_l)^*.$$

现在考虑 LK_l/L, 因为 $(\pi^{-n})^{1/l} \in L$, 故

$$N_{LK_l/L}((\pi^{-n})^{1/l}) = \pi^{-n},$$

因此存在一个 $x_2 \in (LK_l)^*$, 使得

$$\theta(\sigma_\wp) = (\pi^{-n})^{1/l} x_2^{\sigma_\wp - 1}.$$

此处利用了引理 18.5 (3) 及前面类似的推理过程.

由引理 18.5 (4), 有

$$\theta(\sigma_\wp)\theta(\sigma)^{\sigma_\wp} = \theta(\sigma)\theta(\sigma_\wp)^\sigma, \tag{18.12}$$

而 $\sigma_\wp$ 在 $\zeta^{1/l}$ 上的作用是提升 $q = p^f$ 次幂, 因而有

$$\theta(\sigma)^{\sigma_\wp} = ((\zeta^m)^{1/l} x_1^{\sigma-1})^{\sigma_\wp} = \zeta^{mq/l} x_1^{\sigma_\wp\sigma - \sigma_\wp}.$$

σ 在 $\pi^{1/l}$ 上的作用由 $\sigma(\pi^{1/l}) = \zeta\pi^{1/l}$ 给出, 因此有

$$\theta(\sigma_\wp)^\sigma = ((\pi^{-n})^{1/l} x_2^{\sigma_\wp - 1})^\sigma = \zeta^{-n}(\pi^{-n})^{1/l} x_2^{\sigma\sigma_\wp - \sigma}.$$

将以上这些计算代入 (18.12) 式中, 有

$$(\pi^{-n})^{1/l} x_2^{\sigma_\wp - 1} \zeta^{mq/l} x_1^{\sigma\sigma_\wp - \sigma_\wp} = (\zeta^m)^{1/l} x_1^{\sigma-1} \zeta^{-n} (\pi^{-n})^{1/l} x_2^{\sigma\sigma_\wp - \sigma},$$

即

$$\zeta^{-n-m(q-1)/l} = x_1^{\sigma\sigma_\wp - \sigma_\wp - \sigma + 1} x_2^{\sigma - \sigma\sigma_\wp + \sigma_\wp - 1} = \Big(\frac{x_1}{x_2}\Big)^{(\sigma-1)(\sigma_\wp - 1)}.$$

令 $x = \big(\frac{x_1}{x_2}\big)^{\sigma-1}$, 有

$$x^{\sigma_\wp} = \zeta^{-n-m(q-1)/l} x. \tag{18.13}$$

因为我们假定 $\zeta_l \in K$, $\zeta_{l^2} \notin K$, 故 $l|q-1$ 且 $l^2 \nmid q-1$, 即 $l|q-1$ 但 $(q-1)/l \not\equiv 0 \pmod l$, 从而可以计算 $\left(\frac{q-1}{l}\right)^{-1} \pmod l$. 注意到 $(\zeta^{1/l})^{\sigma_\wp}/\zeta^{1/l} = \zeta^{(q-1)/l}$, 从而有

$$\left((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m}\right)^{\sigma_\wp - 1} = \zeta^{-n-m(q-1)/l}.$$

对于 $x/((\zeta^{1/l})^{-((q-1)/l)^{-1}n-m}) = x'$ 而言, 有

$$x'^{\sigma_\wp} = x',$$

此处用到了 (18.13) 式. 可见 $x' \in L$, 从而

$$x = \left(\frac{x_1}{x_2}\right)^{\sigma-1} = (\zeta^{1/l})^{-((q-1)/l)^{-1}n-m}x', \quad x' \in L. \tag{18.14}$$

应用关于 KL_l/K_l 的范映射到 (18.3) 式, 有

$$1 = (\zeta)^{-((q-1)/l)^{-1}n-m}N_{L/K}(x'),$$

此处用到了事实: $(\frac{x_1}{x_2})^{\sigma-1} = x$ 是位于范映射的核中, 因此有

$$\zeta^{-n-m(q-1)/l} \in N_{L/K}(L^*).$$

但是 $\zeta \notin N_{L/K}(L^*)$(否则 $\zeta_{l^2} \in K$), 从而

$$-n - m(q-1)/l \equiv 0 \pmod l$$

即

$$n \equiv -m(q-1)/l \pmod l.$$

这就完成了定理 18.10 的证明. 由于定理 18.10 中的 ψ 的不变量为 n, 所以推论 18.1 是定理 18.10 的直接结论.

§18.4　不变量映射的整体计算

由 §18.2 节知道, 解有限域 $\mathbb{F}_q$ 中群 μ_l 的离散对数问题可转化为局部域上循环代数的不变量计算问题. 在 §18.3 中我们给出了在该局部域中直接计算该循环代数的不变量的上同调方法, 但我们也可以如下考虑这个问题: 由定理 18.9, 有正合列

$$0 \longrightarrow \mathrm{Br}(K) \longrightarrow \bigoplus_{\wp \in S} \mathrm{Br}(K_\wp) \xrightarrow{\sum \mathrm{inv}_\wp} \mathbb{Q}/\mathbb{Z} \longrightarrow 0, \tag{18.15}$$

此处, $\mathrm{Br}(K) \to \bigoplus_{\wp\in S}\mathrm{Br}(K_\wp)$ 由 $A \mapsto \bigoplus_{\wp\in S}(A\bigotimes K_\wp)$ 给出, 而对于 $A_\wp \in \mathrm{Br}(K_\wp)$, 有

$$\left(\sum \mathrm{inv}_\wp\right)\left(\bigoplus_{\wp\in S} A_\wp\right) = \sum_{\wp\in S}\mathrm{inv}_\wp(A_\wp),$$

此处 $\mathrm{inv}_\wp$ 表示 $K_\wp$ 所对应的不变量映射.

现在假定我们的离散对数问题相关到局部域 $K_\wp$ 和 $\mathrm{Br}(K_\wp)$ 中一个元素 $A_\wp$, 为简单起见, 假定 $A_\wp$ 是群 $\mathrm{Br}(K_\wp)$ 中素数阶 l 的元素. 于是我们的任务是有效地计算不变量 $\mathrm{inv}(A_\wp)$. 可更进一步假设 $A_\wp = (L_\wp/K_\wp, \sigma, a_\wp)$, 此处 $L_\wp/K_\wp$ 是 l 次循环扩张, σ 是 $G_\wp = \mathrm{Gal}(L_\wp/K_\wp)$ 的生成元, $a_\wp \in K_\wp^*/N_{L_\wp/K_\wp}(L_\wp^*)$. 为了应用 (18.15) 式来计算 $\mathrm{inv}(A_\wp)$, 我们要将给定的 $A_\wp$ 提升为一个整体代数 A. 然后, 由 (18.15) 式给出的关系

$$\sum_{q\in S}\mathrm{inv}_q(A\otimes K_q) = 0 \quad (在\mathbb{Q}/\mathbb{Z}中) \tag{18.16}$$

表明: 在 $\wp$ 处的不变量 (这是我们感兴趣的) 可以从在其余 $q(\neq \wp)$ 处的不变量得到. 设素理想 q 在 L/K 中非分歧, 也假定整体提升 A 给定, 是一个形式 $(L/K,\sigma,a)$ 的整体循环代数, 由不变量映射的定义, 知道 A 在 q 处的不变量的清晰计算相关到下面两个问题:

(1) 计算 a 的 q-adic 赋值 $v_q(a)$,

(2) 计算一个整数 f_q, 使得 σ^{f_q} 是在 q 处的 Frobenius σ_q.

第 1 个问题不难解决, 例如, 可参见文献 [62] 中的算法 4.8.17. 但第 2 个问题就困难了. 事实上, 我们在 §18.3 中已经看到这个问题是直接相关到有限域中的离散对数问题 (至少我们处理局部 Kummer 扩张的情形如此).

现在假定次数 l 的整体域扩张以及一个形如 $(L/K,\sigma,a)$ 的整体循环代数的存在性, 于是由上面的讨论及 (18.16) 式和定理 18.7 有

$$\sum_{\wp分歧}\mathrm{inv}_\wp(a) + \sum_{q非分歧} f_q v_q(a) \equiv 0 \pmod{l},$$

此处 $\mathrm{inv}_\wp(a)$ 表示 $(L/K,\sigma,a)$ 在 $\wp$ 处的不变量. 因此, 为了计算 $\mathrm{inv}v_\wp(a)$ ($\wp$ 分歧), 我们可以如下进行:

Step 1. 产生一个 l 次扩张, 它在 $\wp$ 处分歧;

Step 2. 固定 K 的 (非分歧) 素理想的一个集合;

Step 3. 生成如下形式的关系式:

$$\sum_{\wp分歧}\mathrm{inv}_\wp(a) + \sum_{q非分歧} f_q v_q(a) \equiv 0 \pmod{l};$$

Step 4. 对 $\text{inv}_\wp(a)$ 和 f_q 解上述齐次线性方程组.

注意一旦完成了上述计算, 则实际上立即解决了两个问题: 第 1, 提供了有限域中离散对数计算的算法; 第 2, 这些算法也计算出了在射类域的某些子域的 Galois 群中一个固定的生成元 σ 和 Frobenius 自同构 σ_q 之间的离散对数. 同时, Brauer 群理论表明: 描述射类域的 Galois 群是密切相关到解有限域中的离散对数问题.

为了完成上述步骤, 从而达到计算不变量的目的, 我们需要知道整体域扩张 L/K 的存在性, 其中 L/K 的扩张次数为素数 l, 且具有预先给定的分歧素理想, 而讨论这些需要整体类域论的有关知识. 下面就叙述一些我们需要的类域论中的结论:

定义 18.5　K 中的一个模数(modulus)m 是一个对 (m_0, m_∞), 其中 m_0 是一个整理想, 而 m_∞ 是 K 到 $\mathbb{C}$ 中实嵌入的一个集合. 我们形式地将其写为 $m = m_0 m_\infty$, 并定义 $(\mathcal{O}/m)^* = (\mathcal{O}/m_0)^* \times \mathbb{F}_2^{m_\infty}$. 若 m 和 n 是两个模数, 且 $m_0 \subset n_0$, $n_\infty \subset m_\infty$, 则称 n 整除 m, 记为 $n|m$. 若 $\mathfrak{a}$ 是一个非零分式理想, 且 $v_\wp(\mathfrak{a}) = 0$ (对所有的 $\wp|m$), 则称 $\mathfrak{a}$ 与 m 互素. 这等价于说 $\mathfrak{a} = \mathfrak{b}/\mathfrak{c}$, 其中 $\mathfrak{b}$ 和 $\mathfrak{c}$ 为整理想且均与 m_0 互素 (在通常意义下). 与 m 互素的分式理想的集合构成一个群, 记为 $I_m(K)$. 若 $\alpha \in K^*$ 且主理想 $\alpha\mathcal{O}_K$ 与 m 互素, 则称 α 与 m 互素.

对于 K 的类群, 有以下熟知的长正合列:

$$1 \longrightarrow U(K) \longrightarrow K^* \longrightarrow I(K) \longrightarrow Cl(K) \longrightarrow 1,$$

其中 $U(K)$ 记 K^* 中单位群, $I(K)$ 记分式 $\mathcal{O}_K$ 理想. 我们希望对 $I_m(K)$ 得出类似的长正合列. 为此, 要定义对应的一些概念.

定义 18.6　设 m 是 K 中一个模数, 对 $\alpha \in K^*$ 及所有 $\wp|m_0$ 和所有嵌入 $\sigma_i \in m_\infty$, 若有 $v_\wp(\alpha - 1) \geqslant v_\wp(m_0)$ 且 $\sigma_i(\alpha) > 0$, 则称 α 模 m 与 1 同余, 记为

$$\alpha \equiv 1 \pmod{m}.$$

定义 $K_m^* = \{\alpha \in K^* | \alpha \equiv 1 \pmod{m}\}$, 而记 $P_m(K)$ 是 K 的所有形如 $\alpha\mathcal{O}_K$ $(\alpha \in K_m^*)$ 的主分式理想的集合, 即 $P_m(K) = \{\alpha\mathcal{O}_K | \alpha \equiv 1 \pmod{m}\}$. 显然, $P_m(K)$ 是 $I_m(K)$ 的一个子群, 称之为 m 的射群. 对于 $P_m(K)$ 中一个元素 $\mathfrak{a}$, 若 $\mathfrak{a} = \alpha\mathcal{O}_K = \beta\mathcal{O}_K$, $\alpha, \beta \in K_m^*$, 则这等价于 α/β 是 K_m^* 中一个单位. 这些单位形成 $U(K)$ 的一个子群, 记为 $U_m(K) = U(K) \cap K_m^*$.

由上面的定义, 我们有下述正合列:

$$1 \longrightarrow U_m(K) \longrightarrow K_m^* \longrightarrow P_m(K) \longrightarrow 1.$$

于是可以类似于类群情形, 定义射类群 $Cl_m(K)$ 如下:

$$1 \longrightarrow P_m(K) \longrightarrow I_m(K) \longrightarrow Cl_m(K) \longrightarrow 1.$$

而下面的定理给出了射类群的有限性及计算其势的公式：

定理 18.11　我们有如下正合列：

$$\begin{aligned} 1 \longrightarrow U_m(K) \longrightarrow U(K) \longrightarrow (\mathcal{O}_K/m)^* \\ \longrightarrow Cl_m(K) \longrightarrow Cl(K) \longrightarrow 1, \end{aligned} \tag{18.17}$$

因此射类群是有限的，并且有

$$h_m(K) = h(K)\frac{|(\mathcal{O}_K/m)^*|}{[U(K):U_m(K)]}, \tag{18.18}$$

此处 $h(K)$ 和 $h_m(K)$ 分别是 $Cl(K)$ 和 $Cl_m(K)$ 的势.

为了叙述整体类域论中的主要定理，我们引进同余子群的概念.

定义 18.7　设 m 是一个模数，如果一个分式理想构成的群 C 满足

$$P_m(K) \subset C \subset I_m(K),$$

则 C 称为模数 m 的一个同余子群. 为了表明 C 是对应于 m 的一个同余子群，我们引入记号 (m, C).

给定一个同余子群 (m, C)，我们有商群 $\overline{C} = C/P_m \subset Cl_m$，从而也可以将一个同余子群视为射类群 Cl_m 的一个子群. 一个自然的问题是：给定 (m_1, C_1) 和 (m_2, C_2)，何时有 $Cl_{m_1}/\overline{C}_1 \cong Cl_{m_2}/\overline{C}_2$？为了回答这个问题，我们引进下面的定义：

定义 18.8　设 (m_1, C_1) 和 (m_2, C_2) 为两个同余子群，若

$$I_{m_2} \cap C_1 = I_{m_1} \cap C_2,$$

则称这两个同余子群是等价的，记为 $(m_1, C_1) \sim (m_2, C_2)$.

易知这是一个等价关系，且当 (m_1, C_1) 和 (m_2, C_2) 等价时，有 $I_{m_1}/C_1 \cong I_{m_2}/C_2$.

定义 18.9　设 m_1 和 m_2 是两个模数，定义 m_1 和 m_2 的最大公因子 $n = \gcd(m_1, m_2) = ((m_{10} + m_{20}), m_{1\infty} \cap m_{2\infty})$. 此处 m_{i0} 和 $m_{i\infty}$ 分别表示 m_i 的整理想部分和无穷远部分. 显然 n 是整除 m_1 和 m_2 的最大模数.

定理 18.12　设 (m_1, C_1) 和 (m_2, C_2) 是两个同余子群且 $(m_1, C_1) \sim (m_2, C_2)$. 令 $n = \gcd(m_1, m_2)$，则存在惟一的同余子群 (n, C)，使得 $(n, C) \sim (m_1, C_1) \sim (m_2, C_2)$，而 $C = C_1P_n = C_2P_n$. 称同余子群 (n, C) 是 (m_1, C_1) 和 (m_2, C_2) 的最大公因子，记为 $C = \mathrm{GCD}(C_1, C_2)$.

现在记 $\mathcal{C}$ 是同余子群的一个等价类，则存在一个同余子群 $(f, C_f) \in \mathcal{C}$，使得 $\mathcal{C}$ 中的每一个元素均具有形式 $(f\mathfrak{a}, C_f \cap I_{f\mathfrak{a}})$，$\mathfrak{a}$ 是 K 中任意模数. 称 (f, C_f) 是 $\mathcal{C}$ 的导子.

定义 18.10 设 (m, C) 为一个同余子群, 考虑与 (m, C) 等价的同余子群构成的等价类 $\mathcal{C}$. 若 (f, C_f) 是 $\mathcal{C}$ 的导子, 则 f 称为 (m, C) 的导子. 而对于任意模数 f, 若存在一个同余子群, 其导子为 f, 则称模数 f 为一个导子.

利用现在的记号, 我们叙述类域论中的主要结果, 它们是定理 4.6 和 4.7 中结果的再叙述. 回顾 Artin 映射的定义

$$\begin{array}{rccc} \mathrm{Art}_{L/K} = (\cdot, L/K): & I_m & \longrightarrow & \mathrm{Gal}(L/K), \\ & \prod\limits_{\wp} \wp^{n_\wp} & \longmapsto & \prod\limits_{\wp} \sigma_\wp^{n_\wp}, \end{array}$$

此处 $\sigma_\wp$ 是 $\wp$ 处的 Frobenius 映射.

定理 18.13 (i) Artin映射是从 I_m 到 G 的一个满同态, 且其核 $A_m(L/K)$ 是相对于 m 的同余子群, 因此Artin映射可视为从 Cl_m 到 G 的满同态.

(ii) 若 $(m_1, A_{m_1}(L_1/K)) \sim (m_2, A_{m_2}(L_2/K))$, 则 L_1 和 L_2 是 K 同构的; 反之对于给定的任意同余子群 (m, C), 一定存在一个Abel扩张 L/K(惟一到 K 同构), 使得 m 是 L/K 的一个合适的模数, 且 $C = A_m(L/K)$.

(iii) Artin映射诱导出一个从 $Cl_m/\overline{C}$ 到 $\mathrm{Gal}(L/K)$ 的典范同构, 且 L/K 的导子 $f = f(L/K)$ 等于对应的同余子群 $A_m(L/K)$ 的导子, 而 K 的在 L 中分歧的位正好就是 $f = f(L/K)$ 的因子.

注意, 这里用到了下面一个概念: 设 m 是 K 的一个模数, L/K 是一个 Abel 扩张, 若 m 是 L/K 的导子 $f = f(L/K)$ 的倍数, 则称 m 是 L/K 的一个合适的模数.

令 $K = \mathbb{Q}$, $\mathbb{Q}$ 的整体类域论由下述 Kronecker-Weber 定理完全决定:

定理 18.14 $\mathbb{Q}$ 的每一个Abel扩张 $K/\mathbb{Q}$ 均包含在某个分圆扩张 $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ 中.

推论 18.2 当且仅当 $l|p-1$ 时, 存在惟一一个次数 l 的、恰好在 p 处分歧的Abel扩张 $K/\mathbb{Q}$.

证明 注意下述显然的事实: 数域 K 在 p 处分歧意味着对每一个包含 K 的分圆域 $\mathbb{Q}(\zeta_n)$, 有 $p|n$, 因此 $\mathbb{Q}(\zeta_p)$ 是包含 K 的最小分圆扩张. $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 的次数为 $p-1$, 因而存在 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 的次数为 l 的一个中间域 K 的充要条件是 $l|p-1$.

由于 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ 是 Galois 的, 且 $(\mathbb{Z}/p\mathbb{Z})^*$ 是循环的, 这样的次数为 l 的中间域是惟一的. 证毕

由此可知 $\mathbb{Q}(\zeta_p)$ 是 $\mathbb{Q}$ 的相对于模数 $m = (p, \infty)$ 的射类域 (因为 $\mathbb{Q}$ 只有一个实嵌入), 也易知射类群同构于 $(\mathbb{Z}/p\mathbb{Z})^* = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 因而射类群的势是 $\phi(p)$. 这也可以由定理 18.11 的公式 (18.18) 得出: 因为 $\mathbb{Z}$ 的单位是 $\{+1, -1\}$, 故 $U_m(\mathbb{Z}) = \{+1\}$, 从而 $[U(\mathbb{Q}) : U_m(\mathbb{Q})] = 2$. 而

$$|(\mathcal{O}_{\mathbb{Q}}/m)^*| = |(\mathbb{Q}/(p))^* \times \mathbb{F}_2| = |(\mathbb{Z}/(p))^*| \cdot 2 = 2\phi(p).$$

利用 (18.18) 式即知射类群的势为 $\phi(p) = p - 1$.

于是我们知道如何计算 $\mathbb{Q}$ 的一个扩张, 使其次数为 l, 且它恰在 p 处分歧: 考虑扩张 $\mathbb{Q}(\zeta_p)/\mathbb{Q}$, 令 $\langle\sigma\rangle = \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$, 然后考虑 $\langle\sigma^l\rangle$ 在 $\mathbb{Q}(\zeta_p)$ 中的固定域 K 即可. 因此, 我们已经确定了次数 l 的恰在一个位上分歧的 $\mathbb{Q}$ 的扩张. 然而, 我们的任务不仅仅是构造这样的扩张, 还要做的事情是在所有非分歧的位上局部地描述其 Galois 群. 我们将通过研究相对 Brauer 群 $\mathrm{Br}(K/\mathbb{Q})$ 来达此目的.

设 $K/\mathbb{Q}$ 如前面所构造, $\langle\sigma\rangle = \mathrm{Gal}(K/\mathbb{Q}) = G$ 是 $K/\mathbb{Q}$ 的 Galois 群, 考虑一个形如 $(K/\mathbb{Q}, \sigma, a)$ 的整体代数 A. 若 $a = \prod q^{n_q}$ 是素分解, 则 Hasse- Brauer-Noether 定理给出如下形式的关系:

$$\mathrm{inv}_p(a) + \sum_{q \neq p} f_q n_q \equiv 0 \pmod{l}. \tag{18.19}$$

现在必须选取一个适当的非分歧素数的集合 $\mathfrak{D}$, 更精确地说, 必须找到一个控制出现在 a 的分解中的素数的办法, 否则每一个新的方程可能就引出新的变量到方程组中. 一个最容易的方法就是将我们的注意力限制在那些只相关到较小素数的、出现在 (18.19) 式中的项, 因而我们很自然地引入自然数的光滑性概念.

下面将给出的算法与经典的有限域中离散对数计算的算法的类似是显而易见的, 而在经典的算法中也用到光滑性的概念.

固定 $\mathbb{F}_p^*$ 的乘法群的一个生成元 g, 注意借助自然约化映射 $a = \prod q^{n_q}$ 也可视为 $\mathbb{F}_p^*$ 中一个元素, 因而考虑 a 相对于基 g 的对数 x, 即惟一决定的自然数 $x \bmod p-1$, 使得 $a \equiv g^x \pmod{p}$. 写 $x = \log_g a$, 于是 $a = \prod q^{n_q}$ 给出方程

$$\log_g a \equiv \log_g \left(\prod q^{n_q}\right) \equiv \sum n_q \log_g(q) \pmod{p-1}.$$

即

$$\log_g a - \sum n_q \log_q \equiv 0 \pmod{p-1}. \tag{18.20}$$

注意 (18.19) 和 (18.20) 式的类似.

下面计算 $K/\mathbb{Q}$ 的 Galois 群的局部性质的方法实际上重新产生了经典的计算 $\mathbb{F}_p$ 中离散对数的指标计算算法. 简单回顾一下它:

开始于元素 $x \in \mathbb{F}_p^*$, 计算 $\log_g(x)$. 为此, 计算 $x^{\exp}$ (对于随机的 exp) 并提升它到 $\overline{x^{\exp}} \in \mathbb{Z}$. 若此提升是光滑的

$$\overline{x^{\exp}} = \prod_{q \in S} q^{n_q},$$

则得到一个如下形式的关系:

$$\exp \cdot \log_g(x) = \sum_{q \in S} n_q \log_g(q) \pmod{p-1}.$$

若能收集到足够的这类关系式, 就可以对 $\log_g(x)$ 和 $\log_g(q)$ 解这个方程组, 从而得出 $\log_g(x)$.

而在 Brauer 群情形, 我们可以完全类比, 一个光滑提升导致一个关系式

$$\exp \cdot \mathrm{inv}_p(x) + \sum_{q \in S} n_q f_q \equiv 0 \pmod{l},$$

从而, 可以计算 $\mathrm{inv}_p(x)$ 和 f_q 如下:

(算法 18.1) $K/\mathbb{Q}$ 的局部性质计算

输入: $x \in \mathbb{F}_p$.

输出: $\mathrm{inv}_p(x)$, f_q.

1. $A := [0]$;
2. $x := \zeta_0$ 到 $\mathbb{F}_p^*$ 的提升;
3. 当 $|A| < |S| - 1$ 时, 选取 $\exp := [1, p-1]$ 中的随机元素, 计算 $\overline{x^{\exp}} = x^{\exp}$ 到 $\mathbb{Z}$ 中的提升, 若 $\overline{x^{\exp}}$ 光滑, 则将 $(\exp, \overline{x^{\exp}})$ 的分解存储, 并将其作为一行添入 A 中;
4. 计算 $\overline{v} := \mathrm{Ker}(A)$ 中元素;
5. 输出 $\overline{v}$.

注意到上述算法与指标计算算法的类似性, 指标计算算法复杂度估计的方法也可以应用到我们的算法. 于是有

定理 18.15　*考虑恰在 p 处分歧的次数 l 的扩张 $K/\mathbb{Q}\,(l|p-1)$, 设 σ 是 $K/\mathbb{Q}$ 的Galois群的生成元, 则计算指数 f_q(使得 $\sigma^{f_q} = \sigma_q$, σ_q 是在 q 处的Frobenius, $q \leqslant L_p(\frac{1}{2}, \rho)$, $\rho \in \mathbb{R}^+$) 具有复杂度*

$$L_p\Big(\frac{1}{2}, \rho + \frac{1}{\rho} + o(1)\Big),$$

此处 $L_N(\alpha, \beta) = \exp(\beta(\log N)^{\alpha}(\log\log N)^{1-\alpha})$.

注意利用上述算法, 就可以计算 $\mathbb{F}_p^*$ 中一个 l 阶循环群中元素 y 关于元素 x 的离散对数. 事实上, 只要能计算出 $\mathrm{inv}_p(y)$ 和 $\mathrm{inv}_p(x)$ 即可, 于是对随机的 $\exp_1$ 和 $\exp_2$, 提升 $x^{\exp_1}y^{\exp_2}$ 到 $\mathbb{Z}$ 并存储由此获得的光滑关系, 计算结果的关系矩阵的核中一个向量, 可得到 $\mathrm{inv}_p(x)$ 和 $\mathrm{inv}_p(y)$. 为了确保从计算出的向量获得 $\mathrm{inv}_p(x)$ 和 $\mathrm{inv}_p(y)$ 的非平凡值, 需要假定矩阵具有最大秩. 在得出 $\mathrm{inv}_p(x)$ 和 $\mathrm{inv}_p(y)$ 后, 所要计算的离散对数即为

$$\mathrm{inv}_p(y)/\mathrm{inv}_p(x) \pmod{l}.$$

下面考虑 $K = \mathbb{Q}(\sqrt{-D})$ 为虚二次域情形.

定理 18.16 设 $K=\mathbb{Q}(\sqrt{-D})(D>0$ 无平方因子且 $D\neq -1,-3)$. 设 m 为伴随到理想 $\mathfrak{a}$ 的一个模数, 则模数 m 的射类群的阶为

$$h_m(K)=h(K)\frac{\phi(\mathfrak{a})}{2}. \tag{18.21}$$

证明 因为 K 是虚二次域, K 没有实嵌入, 从而无实位. 又 $\mathcal{O}_K$ 的单位群为 $\{+1,-1\}$, 因此 $U_m(K)=\{+1\}$. 利用定理 18.11 中的公式 (18.18), 有

$$h_m(K)=h(K)\doteq\frac{|(\mathcal{O}_K/m)^*|}{[U(K):U_m(K)]}=h(K)\frac{|(\mathcal{O}_K/\mathfrak{a})^*|}{2}=h(K)\frac{\phi(\mathfrak{a})}{2}.$$

定理得证.

推论 18.3 设 $\wp$ 是 K 中一素理想, 且 $l|N_{K/\mathbb{Q}}(\wp)-1$, $l\neq 2$ 为素数, 又设 $(l,h(K))=1$, 则存在一个 l 次扩张 L/K, 它恰在 $\wp$ 处分歧.

固定 K 上一个恰在 $\wp$ 处分歧的 l 次扩张 L, 令 $\mathrm{Gal}(L/K)=\langle\sigma\rangle$, 与前面 $K=\mathbb{Q}$ 的情形一样, 我们想局部地描述 $\mathrm{Gal}(L/K)$. 即：对于在 L/K 中惰性的一个素理想 $\mathfrak{q}\subset K$, 找出 σ 和 $\sigma_{\mathfrak{q}}$ 之间的关系. 为了获得我们感兴趣的有关指数 $f_{\mathfrak{q}}$ 的信息, 应用 $K/\mathbb{Q}$ 的算法. 考虑一个整体循环代数 $(L/K,\sigma,q)$, q 为一有理素数, 它给出一个关系式

$$\mathrm{inv}_{\wp}(q)+\sum_{\mathfrak{q}|q}f_{\mathfrak{q}}\equiv 0 \pmod{l}.$$

但是 $\mathrm{inv}_{\wp}(q)$ 对应到局部循环代数 $(L_{\wp}/K_{\wp},\sigma,q)$, 此处 q 必须视为 $k_{\wp}^*/k_{\wp}^{*l}\cong\mathbb{F}_{p^2}^*/\mathbb{F}_{p^2}^{*l}$ 中元素 (引理 18.4). 假定 q 在这个商中是平凡的, 则有 $\mathrm{inv}_{\wp}(q)\equiv 0 \pmod{l}$, 由此可知：若 $q=\mathfrak{q}_1\mathfrak{q}_2$ 在 K 中分裂, 则 $f_{\mathfrak{q}_1}\equiv -f_{\mathfrak{q}_2} \pmod{l}$; 若 q 是惰性的, 则 $f_{\mathfrak{q}}\equiv 0$. 从而有

定理 18.17 若 q 在 $K/\mathbb{Q}$ 中是惰性的 (即 $(q)=\mathfrak{q}$), 且 q 在 $k_{\wp}$ 中的阶与 l 互素, 则 $f_{\mathfrak{q}}=0$; 若 q 在 $K/\mathbb{Q}$ 中分裂 (即 $q=\mathfrak{q}\bar{\mathfrak{q}}$), 且 q 在 $k_{\wp}$ 中的阶与 l 互素, 则 $f_{\mathfrak{q}}\equiv -f_{\bar{\mathfrak{q}}} \pmod{l}$.

推论 18.4 设 $l|p+1$, 则有

(i) 若 $q\mathcal{O}_K=\mathfrak{q}$, 则 $f_{\mathfrak{q}}=0$;

(ii) 若 $q\mathcal{O}_K=\mathfrak{q}\bar{\mathfrak{q}}$, 则 $f_{\mathfrak{q}}\equiv -f_{\bar{\mathfrak{q}}} \pmod{l}$.

现在设 $l|p+1$, 对 $a\in K$, 令

$$a\mathcal{O}_K=\prod_{\mathfrak{q}\text{惰性}}\mathfrak{q}^{m_{\mathfrak{q}}}\prod_{\mathfrak{q}\text{分裂}}\mathfrak{q}^{n_{\mathfrak{q}}}\bar{\mathfrak{q}}^{n_{\bar{\mathfrak{q}}}},$$

应用推论 18.4 来局部地描述 Galois 群 $\mathrm{Gal}(L/K)$：考虑来自代数 $(L/K,\sigma,a)$ 的关系, 有

$$\mathrm{inv}_{\wp}(a)\equiv\sum_{\mathfrak{q}\text{惰性}}f_{\mathfrak{q}}m_{\mathfrak{q}}+\sum_{\mathfrak{q}\text{分裂}}(f_{\mathfrak{q}}n_{\mathfrak{q}}+f_{\bar{\mathfrak{q}}}n_{\bar{\mathfrak{q}}}) \pmod{l}. \tag{18.22}$$

由前面讨论知, 对 q 在 K 中为惰性的, $f_{\mathfrak{q}} \equiv 0 \pmod{l}$, 而对 q 为分裂的, 则计算 $f_{\mathfrak{q}}$ 就够了, 因为 $f_{\overline{\mathfrak{q}}} \equiv -f_{\mathfrak{q}} \pmod{l}$. 因此, 可以化简 (18.22) 式的关系: 去掉所有惰性素数, 用 $f_{\mathfrak{q}}(n_{\mathfrak{q}} - n_{\overline{\mathfrak{q}}})$ 代替 $f_{\mathfrak{q}}n_{\mathfrak{q}} + f_{\overline{\mathfrak{q}}}n_{\overline{\mathfrak{q}}}$, 有

$$\mathrm{inv}_{\wp}(a) + \sum_{\mathfrak{q}\text{分裂}} (f_{\mathfrak{q}}(n_{\mathfrak{q}} - n_{\overline{\mathfrak{q}}})) \equiv 0 \pmod{l}. \tag{18.23}$$

于是我们有以下算法:

(算法 18.2) 计算 $\mathbb{F}_{p^2}$ 中 l 阶循环群的离散对数 ($l|p+1$)

输入: $\mathbb{Q}(\sqrt{-D})$, D 无平方因子, $D \neq -1, -3$; $a, b \in \mathbb{F}_{p^2}$.

输出: 整数 n, 使 $\left(a^{(p^2-1)/l}\right)^n = b^{(p^2-1)/l}$.

1. 生成有理素数 $p \leqslant B$ 构成因子基 S_{rat};

2. 生成代数因子基 S_{alg}(对于在 K 中分裂的有理素数 q, S_{alg} 只包含分解 $q = \mathfrak{q}\overline{\mathfrak{q}}$ 中的一个素理想, 比如说 $\mathfrak{q}$);

3. 在 $\mathbb{F}_{p^2}$ 中计算 $x = a^{n_a}b^{n_b}$;

4. 提升 x 到 K 中一个元素 $\overline{x}$;

5. 若 $N_{K/\mathbb{Q}}(\overline{x})$ 是 B- 光滑的, 分解

$$\overline{x}\mathcal{O}_K = \prod_{s\text{惰性}} s^{n_s} \prod_{q\text{分裂}} \mathfrak{q}^{n_{\mathfrak{q}}}\overline{\mathfrak{q}}^{n_{\overline{\mathfrak{q}}}};$$

6. 存储关系式 $(n_a, n_b, n_{\mathfrak{q}} - n_{\overline{\mathfrak{q}}})_{\mathfrak{q}\in S_{\text{alg}}}$;

7. 一旦收集到足够多 ($> |S_{\text{alg}}| + 2$) 个关系式, 就建立矩阵 A;

8. 计算 $v = \ker(A)$;

9. 输出 $v_2/v_1 \pmod{l}$.

注意, 此处的代数因子基 S_{alg} 是从 S_{rat} 生成的, 对于 S_{rat} 中所有惰性素数, 全部略去不要, 而对 S_{rat} 中的分裂素数 $q = \mathfrak{q}\overline{\mathfrak{q}}$, 仅取其一作为 S_{alg} 的元素. 因此, 代数因子基 S_{alg} 元素个数正好为 S_{rat} 元素个数的一半, 从而上述算法相比较经典情形的指标计算更容易了.

利用文献 [63] 的方法, 可估计上述算法 18.2 的复杂度, 我们有

定理 18.18　*设 $K = \mathbb{Q}(\sqrt{-D})$ 为虚二次数域, $\wp$ 是 K 中位于惰性有理素数 p 上的素理想, 设 l 为素数, $l|p+1$. 假定 L/K 是恰在 $\wp$ 处分歧的 l 次扩张, σ 是 $\mathrm{Gal}(L/K)$ 的一个生成元, 则对于范数界于 $L_p(1/2, \sqrt{4/3})$ 的素理想 $\mathfrak{q}$, 计算指数*

$f_{\mathfrak{q}}$(即使得 $\sigma^{f_{\mathfrak{q}}}$ 等于 $\mathfrak{q}$ 处的Frobenius $\sigma_{\mathfrak{q}}$ 的整数 $f_{\mathfrak{q}}$) 的复杂度为

$$L_p(1/2, \sqrt{48} + o(1)).$$

下面考虑 $l|p-1$ 的情形, 此时 p 在 $K/\mathbb{Q}$ 中可以是惰性的或者分裂的. 先设 p 是惰性的, 则 $p\mathcal{O}_K = \wp$. 此时, 在上述算法 18.2 中的代数因子基必须包括惰性的和分裂素理想 (因为我们不能应用定理 18.17). 于是从整体代数 $(L/K, \sigma, a)$(此处 L/K 记在属于 $\wp$ 的射类域中的次数 l 的扩张), 获得如下形式的关系:

$$\mathrm{inv}_{\wp}(a) + \sum_{q\text{惰性}} f_{\mathfrak{q}} v_{\mathfrak{q}}(a) + \sum_{q\text{分裂}} (f_{\mathfrak{q}} v_{\mathfrak{q}}(a) + f_{\overline{\mathfrak{q}}} v_{\overline{\mathfrak{q}}}(a)) \equiv 0 \pmod{l}.$$

因为 S_{rat} 中正好一半元素在 L/K 中是惰性的, 而另一半在 L/K 中是分裂的, 故 S_{alg} 的尺度大小为 $\frac{3}{2}|S_{\mathrm{rat}}|$. 因而应用这个方法计算 $\mathbb{F}_p^*$ 中的 l 阶子群的离散对数并没有什么优势.

现在假设 $p = \wp_1\wp_2$ 在 $K/\mathbb{Q}$ 中分裂, 这意味着多项式 $f(x) = x^2 + D$ 在模 p 后分裂成 $(x - x_1)(x - x_2)$ 的形式. 注意到若记 α 是 $f(x)$ 的一个整体根, 它生成 $K/\mathbb{Q}$, 则 $a + b\alpha\ (a, b \in \mathbb{Z})$ 在 $\wp_1$ 和 $\wp_2$ 的剩余类域中分别对应到局部的元素 $a + bx_1$ 和 $a + bx_2$. 现在设 L/K 是模数 $m = \wp_1$ 的射类域, 则 L/K 恰在 $\wp_1$ 处分歧. 于是来自整体代数 $(L/K, \sigma, a + b\alpha)$ 的关系式如下:

$$\mathrm{inv}_{\wp_1}(a + bx_1) + \sum_{\mathfrak{q} \neq \wp_1} f_{\mathfrak{q}} v_{\mathfrak{q}}(a + b\alpha) \equiv 0 \pmod{l}. \tag{18.24}$$

假定 $a + bx_1$ 和 $a + b\alpha$ 均是光滑的, 即 $a + b\alpha$ 的范数关于某个代数因子基 S_2 是光滑的, 而 $a + bx_1 \in \mathbb{F}_p$ 可以提升为 $\mathbb{Z}$ 中一个元素 β, β 关于某个有理因子基 S_1 是光滑的, 令

$$a + bx_1 = \prod_{q \in S_1} q^{n_q}, \qquad a + b\alpha = \prod_{\mathfrak{q} \in S_2} \mathfrak{q}^{n_{\mathfrak{q}}},$$

则关系式 (18.24) 可重新写为如下形式:

$$\sum_{q \in S_1} n_q \mathrm{inv}_{\wp_1}(q) + \sum_{\mathfrak{q} \in S_2} f_{\mathfrak{q}} v_{\mathfrak{q}}(a + b\alpha) \equiv 0 \pmod{l}.$$

搜寻对 $(a, b) \in \mathbb{Z}^2$, 使得 $a + bx_1$ 和 $a + b\alpha$ 是光滑的. 如果我们收集到足够多的这种对, 则可以解所得方程组而得到 $\mathrm{inv}_{\wp_1}(q)$, $q \in S_1$ 和 $f_{\mathfrak{q}}$, $\mathfrak{q} \in S_2$. 这正好就是所谓高斯整数筛法的推广情形, 这是素域 $\mathbb{F}_p$ 中离散对数问题最有效的已知方法, 例如, 参见文献 [64].

注记 18.1 由本节的讨论, 我们知道 $\mathbb{F}_p$ 中离散对数问题求解的经典指标计算方法及更精细的高斯整数方法, 都可以描述为某个数域的射类域的 Galois 群的局

部不变量的计算. 在下一节中, 我们将看到更高级的数域筛法和函数域筛法也可以如此描述, 从而有限域上所有已知的离散对数计算的有效算法均可以用 Brauer 群理论统一起来.

下面看两个例子, 其中第 1 例是利用算法 18.1, 而第 2 个例子则是利用算法 18.2.

例 18.1　设 $p=10^{15}+37$, 考虑 $\mathbb{F}_p^*$ 中 37 阶循环子群的离散对数问题. 令

$$\zeta_0=627390197251587,\quad \zeta_1=312088005699472,$$

这是 $\mathbb{F}_p$ 中两个 37 次单位根. 它们在 $\mathbb{F}_p$ 的提升是 $x_0=23$ 和 $x_1=57$, 即

$$\zeta_0=x_0^{(p-1)/37},\quad \zeta_1=x_1^{(p-1)/37}.$$

考虑 $\mathbb{Q}$ 的恰在 $p=10^{15}+37$ 处分歧的 37 次扩张. 我们选取所有到 1009 的所有素数作为因子基 S, 在 $\mathbb{F}_p^*$ 中搜寻元素 $23^{k_1}37^{k_2}$, 使其在 $\mathbb{Z}$ 上的提升可在 S 上分解, 其中 k_1 和 k_2 是区间 $[1,p]$ 上的随机整数. 在搜索到 200 个光滑提升后, 我们得到所要的关系矩阵, 这个矩阵是从 200 个形如

$$\sum_{q_i\in S}n_if_i+k_1\mathrm{inv}_p(\zeta)+k_2\mathrm{inv}_p(\zeta^n)=0$$

的列得出的. 最后的线性方程有 167 个变量, 秩为 166, 而其核由下述向量生成:
(1, 8, 31, 20, 32, 18, 23, 7, 29, 25, 5, 36, 11, 12, 7, 9, 14, 32, 4, 14, 27, 14, 35, 35, 12, 34, 5, 27, 19, 17, 17, 15, 15, 20, 22, 16, 2, 33, 15, 35, 26, 34, 34, 6, 23, 4, 5, 12, 11, 33, 33, 29, 10, 33, 30, 15, 1, 3, 2, 5, 20, 28, 6, 28, 3, 20, 9, 29, 23, 18, 30, 26, 20, 4, 6, 24, 1, 27, 9, 17, 14, 25, 14, 7, 13, 13, 2, 19, 13, 6, 9, 21, 4, 31, 1, 27, 23, 18, 24, 19, 4, 12, 29, 13, 27, 10, 7, 14, 5, 28, 1, 31, 14, 2, 28, 28, 4, 35, 15, 31, 19, 6, 19, 9, 10, 2, 5, 12, 36, 34, 24, 34, 10, 8, 30, 28, 11, 35, 11, 33, 26, 34, 25, 24, 1, 21, 34, 27, 18, 7, 9, 26, 25, 19, 29, 2, 15, 30, 26, 3, 5, 22, 17, 13, 21, 8, 22).
其中最后两项对应要求的两个不变量, 由于 $22/8\equiv 12 \pmod{37}$, 故所求离散对数为 12. 事实上, 直接验算知 $\zeta_0^{12}=\zeta_1$ (在 $\mathbb{F}_p$ 中).

例 18.2　考虑 $\mathbb{F}_{151^2}$ 中 19 阶循环子群的离散对数, 应用整体数域 $K=\mathbb{Q}(\sqrt{-31})$, 易知 $h(K)=3$. 由于 $19|151+1$, 我们可以应用算法 18.2. 令 $\zeta_0=136z+24$, $\zeta_1=69z+36$, 其中 z 记多项式 x^2+31 在 $\mathbb{F}_{151^2}$ 中的一个根. $\zeta_0=(3z+1)^{(151^2-1)/19}$, $\zeta_1=(40z+80)^{(151^2-1)/19}$, 即 ζ_0 和 ζ_1 分别是伴随到 $3z+1$ 和 $40z+80$ 的 19 次单位根. 我们想求 ζ_1 关于 ζ_0 的离散对数. 选取位于 2, 5 和 7 上的素理想 $\wp_{2,1}$, $\wp_{5,1}$,

$\wp_{7,1}$ 作为因子基 S. 我们搜索到以下光滑关系式:

$$(3z+1)^1=(3z+1)\longrightarrow(3\sqrt{-31}+1)\mathcal{O}_K=\wp_{2,1}^1\wp_{2,2}^2\wp_{5,1}^1\wp_{7,1}^1,$$

$$(3z+1)^{156}=(6z+102)\longrightarrow(6\sqrt{-31}+102)\mathcal{O}_K=\wp_{2,1}^6\wp_{2,2}^2\wp_{5,1}^1,$$

$$(3z+1)^{170}=(128z+128)\longrightarrow(128\sqrt{-31}+128)\mathcal{O}_K=\wp_{2,1}^{11}\wp_{2,2}^8,$$

$$(3z+1)^{181}=(12z+116)\longrightarrow(12\sqrt{-31}+116)\mathcal{O}_K=\wp_{2,1}^3\wp_{2,2}^6\wp_{5,2}^1\wp_{7,1}^1,$$

$$(3z+1)^{253}=(12z+52)\longrightarrow(12\sqrt{-31}+52)\mathcal{O}_K=\wp_{2,1}^3\wp_{2,2}^7\wp_{7,2}^1,$$

于是获得下面的线性方程组:

$$\begin{aligned}
\mathrm{inv}_{\wp}(3z+1)-f_2+f_5+f_7&\equiv0\pmod{19},\\
156\mathrm{inv}_{\wp}(3z+1)+4f_2+f_5&\equiv0\pmod{19},\\
170\mathrm{inv}_{\wp}(3z+1)+3f_2&\equiv0\pmod{19},\\
181\mathrm{inv}_{\wp}(3z+1)-3f_2-f_5+f_7&\equiv0\pmod{19},\\
253\mathrm{inv}_{\wp}(3z+1)-4f_2-f_7&\equiv0\pmod{19}.
\end{aligned}$$

上述方程组的一组解为 $\mathrm{inv}_{\wp}(3z+1)\equiv1, f_2\equiv13, f_5\equiv1, f_7\equiv11 \pmod{19}$. 因为

$$(40\sqrt{-31}+80)\mathcal{O}_K=\wp_{2,1}^3\wp_{2,2}^3\wp_{5,1}^2\wp_{5,2}^1\wp_{7,2}^1,$$

故有

$$\mathrm{inv}_{\wp}(40z+80)+f_5-f_7\equiv0\pmod{19},$$

于是 $\mathrm{inv}_{\wp}(40z+80)\equiv10 \pmod{19}$. 因此所求的离散对数应该是 10. 直接验算知道 $\zeta_0^{10}=\zeta_1$.

§18.5 数域筛法

上一节考虑了素域 $\mathbb{F}_p$ 上的离散对数问题. 本节将考虑一般有限域 $\mathbb{F}_{p^n}$ 上的离散对数问题. 为了更好地理解将要叙述的方法的动机, 我们回顾一下素域 $\mathbb{F}_p^*$ 中 l 阶循环子群的离散对数的计算方法. 假定给定了两个元素 $a,b\in\mathbb{F}_p^*$, 它们伴随到两个 l 次单位根 $\zeta_a=a^{(p-1)/l}$, $\zeta_b=b^{(p-1)/l}$. 为了计算 ζ_a 和 ζ_b 之间的离散对数, 我们如下进行:

随机生成对 (r,s), 计算 $c\equiv a^rb^s \pmod p$, 若 c 到 $\mathbb{N}$ 的提升是光滑的 (即在某个因子基 S 上可分解), 则存储 (r,s,c). 若能生成足够多的三元组 $(r_i,s_i,c_i)_{i=1,2,\cdots,t}$, 则可找到整数 $e_1,\cdots,e_t$, 使得

$$\prod_{i=1}^{t}c_i^{e_i}=x^l,\quad x\in\mathbb{Z}.$$

事实上, 考虑分解 $c_i = \prod_{j=1}^{|S|} p_j^{n_{ji}}$, 则

$$\prod_{i=1}^{t} c_i^{e_i} = \prod_{j=1}^{|S|} p_j^{\sum\limits_{i=1}^{t} n_{ji} e_i}.$$

若 $\sum_{i=1}^{t} n_{ji} e_i \equiv 0 \pmod{l}$ 对所有 j 成立, 则 $\prod_{i=1}^{t} c_i^{e_i}$ 是一个 l 次幂. 因此, 要找到下述方程组的一个非平凡解:

$$\begin{cases} n_{11}e_1 + n_{12}e_2 + \cdots + n_{1t}e_t \equiv 0 & \pmod{l}, \\ \qquad\cdots & \\ n_{|S|1}e_1 + n_{|S|2}e_2 + \cdots + n_{|S|t}e_t \equiv 0 & \pmod{l}. \end{cases}$$

若 $t > |S|$, 则非平凡的解存在, 于是得到

$$a^{k_a} b^{k_b} = x^l \quad (\text{在 } \mathbb{F}_p \text{ 中}),$$

此处 $k_a = \sum_{i=1}^{t} e_i r_i$, $k_b = \sum_{i=1}^{t} e_i s_i$. 于是离散对数由 $-k_a/k_b \pmod{l}$ 给出 (假定 $k_b \pmod{l}$ 是可逆的).

现在将上述想法推广到 $\mathbb{F}_{p^n}$ 上, 看会有什么情形发生? 为此取一个 n 次数域 $K/\mathbb{Q}$, 设 p 在 K 中是惰性的, 从而 $p\mathcal{O}_K = \wp$ 为 K 中素理想. 于是 $\mathbb{F}_{p^n}$ 可表示为 $\mathcal{O}_K/\wp\mathcal{O}_K$, $\mathcal{O}_K$ 记 K 的整数环. 假定 $a, b \in \mathbb{F}_{p^n}$, $l | p^n - 1$, 则 $\zeta_a = a^{(p^n-1)/l}$ 和 $\zeta_b = b^{(p^n-1)/l}$ 是两个 l 次单位根. 我们欲求 ζ_a 和 ζ_b 之间的离散对数. 类似 $\mathbb{F}_p$ 的情形, 随机生成对 (r, s) 并计算 $c = a^r b^s \in \mathbb{F}_{p^n}$. 由于同构 $\mathcal{O}_K/\wp\mathcal{O}_K \cong \mathbb{F}_{p^n}$, 故可以提升 c 到 $\mathcal{O}_K$ 中一个元素. 若 $c\mathcal{O}_K$ 可在由 K 的素理想组成的一个代数因子基 S 上分解 (即 $c\mathcal{O}_K$ 关于代数因子基光滑), 则存储 (r, s, c). 假定可以找到足够多的三元组 (r_i, s_i, c_i) $(1 \leqslant i \leqslant t)$, 则类似地可找到整数 e_i, 使得

$$\left(\prod_{i=1}^{t} c_i^{e_i}\right)\mathcal{O}_K = I^l, \tag{18.25}$$

此处 I 是 $\mathcal{O}_K$ 中某个理想. 但是现在不能应用素域时的推理, 因为理想 I 不一定是主理想!

这就导致了下述数论问题:

定义 18.11　令

$$V_l = \{\alpha \in K \mid v_\wp(\alpha) \equiv 0 \pmod{l}, \ \forall \wp\},$$

则称决定 V_l/K^{*l} 中一个元素是否为平凡的这个问题为障碍问题.

如果能找到一个方法解决上述障碍问题, 则下述算法就给出了计算 ζ_a 和 ζ_b 的离散对数问题的一个方法:

(算法 18.3) 计算 $\mathbb{F}_{p^n}^*$ 中 l 阶循环子群的离散对数

输入： 有限域 $\mathbb{F}_p^n$, 数域 K, 满同态 $\phi: \mathcal{O}_K \to \mathbb{F}_{p^n}$, $a, b \in \mathbb{F}_{p^n}$.

输出： 整数 m, 使得 $\zeta_a^m = \zeta_b$.

1. 选择代数数域 K 中素理想构成的某个因子基 S;
2. 随机生成 $c = a^{S_a} b^{S_b}$, 借助于 ϕ 提升 c 到 $\mathcal{O}_K$ 中元素 $\bar{c}$, 若 $\bar{c}$ 是 S 光滑的, 则存储 $\bar{c}$;
3. 找出多于 $|S|$ 个的光滑提升 $\bar{c}_1, \bar{c}_2, \cdots, \bar{c}_t (c_i = a^{S_{a_i}} b^{S_{b_i}}, 1 \leqslant i \leqslant t)$;
4. 计算 $e_i \in \mathbb{Z}/l\mathbb{Z}$, 使得 $\left(\prod_{i=1}^t \bar{c}_i^{e_i}\right)\mathcal{O}_K = I^l$;
5. 决定 $\left(\prod_{i=1}^t \bar{c}_i^{e_i}\right)$ 是否为 K 中一个 l 次幂;
6. 若是, 则输出 $(-\sum e_i S_{a_i})/(\sum e_i S_{b_i}) \pmod{l}$.

于是, 我们需要研究障碍问题. 目前对此问题有两种处理方法. 第 1 种是 Adleman 和 Demarrais 给出的特征签名方法, 而第 2 种是 Schirokauer 给出的基于 p-adic 对数的技术. 下面简单回顾一下这两种方法.

首先介绍特征签名的概念. 该概念最开始是为了分解因子而发展出来的, 而后由 Adleman 在文献 [65] 中引进到指标计算算法中.

设 K 是一个数域, 若一个代数整数 $\alpha \in \mathcal{O}_K$ 生成形如 I^l 的理想 (其中 I 为 $\mathcal{O}_K$ 中一个理想, l 为正整数), 则 α 称为关于 $\mathcal{O}_K$ 的 l 奇异整数. 假设 σ, τ 是两个 l 奇异整数, 若存在 $\alpha, \beta \in \mathcal{O}_K$, 使得 $\alpha^l \sigma = \beta^l \tau$, 则称 σ 等价于 τ. 令 $G(l)$ 是 l 奇异整数关于这个等价关系的等价类构成的群. 它是一个指数整除 l 的, 具有单位 $I(l) = \{\alpha^l | \alpha \in \mathcal{O}_K\}$ 的群, 其群运算定义为

$$[\alpha][\beta] \longmapsto [\alpha\beta].$$

令 $Cl(K)[l]$ 是 K 的类群的 l-torsion 部分, 则 $G(l)$ 可写成如下形式:

$$G(l) \cong U(K)/U(K)^l \oplus Cl(K)[l], \tag{18.26}$$

其中 $U(K)$ 记 K 的单位群. 下面引进特征签名的概念:

考虑 $\mathcal{O}_K$ 的素理想 $\wp_1, \cdots, \wp_t$, 元素 $n_1, \cdots, n_t \in \mathcal{O}_K$, $\sigma \in \mathcal{O}_K$. 假定 $(\sigma) + \wp_i = (1)$, $\forall i$, 且 $l | N(\wp_i) - 1$, n_i 是 $(\mathcal{O}_K/\wp_i)^*$ 中的 l 次本原单位根, 则 σ 关于 $\langle \wp_i, n_i \rangle$ 的特征签名是 $\langle e_1, \cdots, e_t \rangle$, 此处

$$\sigma^{(N(\wp_i)-1)/l} \equiv n_i^{e_i} \pmod{\wp_i}.$$

假定 $K/\mathbb{Q}$ 是 Abel 扩张, 则由 Cebotarev 定理可知, 对所有素理想 $\wp_i$ 和 $c \in G(l)$, 存在 $\sigma \in \mathcal{O}_K$, 使得 $[\sigma] = c$ 且 $(\sigma) + \wp_i = (1)$.

给定 $c \in G(l)$ 和 $\langle \wp_i, n_i \rangle$, 定义映射 θ 如下：θ 将 c 映到 σ 关于 $\langle \wp_i, n_i \rangle$ 的特征签名, 此处 $\sigma \in \mathcal{O}_K$, 使得 $[\sigma] = c$ 且 $(\sigma) + \wp_i = (1)$. 可以证明 θ 是 $G(l)$ 上良好定义的, 且是一个群同态

$$\theta:\ G(l) \longrightarrow \bigoplus_{i=1}^{t} \mathbb{Z}/l\mathbb{Z}.$$

利用这些性质可以解决障碍问题. 由于类数有限性和 $U(K)$ 的有限生成性, 由 (18.26) 式知 $G(l)$ 是有限生成的. 令 H 是 $G(l)$ 的生成元的数目, 则利用算法 18.3 中第 1~4 步 H 次, 容易构造出 H 个 l 奇异整数 $(\sigma_i)_{i=1,2,\cdots,H}$. 计算元素 σ_i 的特征签名 θ_i, 并找出元素 b_i, 使得

$$\sum_i b_i\theta_i \equiv \langle 0, \cdots, 0 \rangle \pmod{l}.$$

而 Adleman 论证了映射 $\theta: G(l) \to \oplus\mathbb{Z}/l\mathbb{Z}$ 很可能是一个单射, 因此这些 σ_i 和 b_i 实际上产生出 $G(l)$ 中的恒等元. 即存在 $\delta \in \mathcal{O}_K$, 使得

$$\prod_i \sigma_i^{b_i} = \delta^l.$$

于是我们遇到的障碍问题得到了解决.

现在介绍 Schirokauer 在文献 [43] 中给出的解决障碍问题的方法.

设 K 是一个数域, l 是一个有理素数, 它在 K 中不分歧. 令

$$\Gamma_1 = \{\gamma \in \mathcal{O}_K | N_{K/\mathbb{Q}}(\gamma) \not\equiv 0 \pmod{l}\}.$$

对 $\mathcal{O}_K$ 中每个整除 (l) 的素理想 L, 令 $\varepsilon_L = |(\mathcal{O}_K/L)^*|$, 并令 ε 是 ε_L 的最小公倍数, 则对所有 $\gamma \in \Gamma_1$, 有

$$\gamma^{\varepsilon} \equiv 1 \pmod{l}.$$

现定义

$$\begin{aligned} \lambda_1:\ \Gamma_1 &\longrightarrow l\mathcal{O}_K/l^2\mathcal{O}_K, \\ \gamma &\longmapsto (\gamma^{\varepsilon} - 1) + l^2\mathcal{O}_K. \end{aligned}$$

对于 $i > 1$, 令 $\Gamma_i = \{\gamma \in \Gamma_{i-1} | \lambda_{i-1}(\gamma) = 0\}$, $\lambda_i : \Gamma_i \to l^{2^{i-1}}\mathcal{O}_K/l^{2^i}\mathcal{O}_K$ 是如下定义的函数：$\lambda_i(\gamma) = (\gamma^{\varepsilon} - 1) + l^{2^i}\mathcal{O}_K$. 对于 $1 \leqslant j \leqslant n$, 设 $\{b_j l^{2^{i-1}} + l^{2^i}\mathcal{O}_K\}$ 是 $l^{2^{i-1}}\mathcal{O}_K/l^{2^i}\mathcal{O}_K$ 在 $\mathbb{Z}/l^{2^{i-1}}\mathbb{Z}$ 上的一组 (模) 基, 则 λ_i 由映射

$$\lambda_{i,j}:\ \Gamma_i \longrightarrow \mathbb{Z}/l^{2^{i-1}}\mathbb{Z}$$

给出, 此处 $\lambda_{i,j}$ 由下述同余式给出:

$$\gamma^{\varepsilon}-1\equiv\sum_{j=1}^{n}\lambda_{i,j}(\gamma)b_j l^{2^{i-1}}\pmod{l^{2^i}}.$$

由于 $\lambda_i(\gamma\gamma')=\lambda_i(\gamma)+\lambda_i(\gamma')$, $\lambda_{i,j}(\gamma\gamma')=\lambda_{i,j}(\gamma)+\lambda_{i,j}(\gamma')$, 这些映射定义了 $\mathcal{O}_K$ 的单位群上的同态.

这些映射 λ_i 和障碍问题之间的关系由下述定理得知:

定理 18.19　*设 e 是一个正整数, ρ 是使得 $2^\rho>e$ 的最小整数. 假定 K 的类数不被 l 整除, 且 $\mathcal{O}_K$ 中模 l^{e+1} 同余于 1 的单位均是 l^e 次幂. 设 $\gamma\in\Gamma_\rho$, 使得 $\mathrm{ord}_\wp(\gamma)\equiv 0\pmod{l^e}$(对所有 $\mathcal{O}_K$ 中素理想 $\wp$ 成立) 且 $\lambda_\rho(\gamma)=0$, 则 γ 是 $\mathcal{O}_K$ 中一个 l^e 次幂.*

证明见引理 15.5 和上面给出的 Schirokauer 的文章 [43].

上面给出的两种方法可以用来解决障碍问题. 下面考虑 Brauer 群在这个问题中的应用. 我们做出下面的基本假定:

基本假定　假定存在 $\mathcal{O}_K$ 中一个素理想 $\wp$, 使得 k 包含在 $\wp$ 的剩余类域中, 设 $K_\wp$ 是 K 的属于模数 $m=\wp$ 的射类域, 假设 $Cl_m(K)$ 的阶被 l 整除且 $(h(K),l)=1$.

由于上述假定, 我们有 $l||\mathrm{Gal}(K_\wp/K)|$. 由于 $\mathrm{Gal}(K_\wp/K)$ 是交换的, 故可以找到一个阶为 $|\mathrm{Gal}(K_\wp/K)|/l$ 的子群 H, 它固定一个次数为 l 的 Galois 扩张 L/K. 由于 $(h(K),l)=1$, 该扩张必定在 $\wp$ 处分歧 (因为它不能包含在 K 的 Hilbert 类域中). 考虑形如 $(L/K,\sigma,a)$ 的整体代数. 下面的引理是至关重要的:

引理 18.6　*设 $a\in K$ 是 $V_l=\{\alpha\in K^*|\ l|v_\mathfrak{q}(\alpha),\forall\mathfrak{q}\}$ 中一个元素, 则在上述基本假定下, 有 $\mathrm{inv}_\wp(a)\equiv 0\pmod{l}$.*

证明　考虑来自整体代数 $(L/K,\sigma,a)$ 的关系, 有

$$\mathrm{inv}_\wp(a)+\sum_{\mathfrak{q}\neq\wp}f_\mathfrak{q}v_\mathfrak{q}(a)\equiv 0\pmod{l}.\tag{18.27}$$

由于 $a\in V_l$, 故 $l|v_\mathfrak{q}(a)$, 即 (18.27) 式的和式中每一项均为零, 从而 $\mathrm{inv}_\wp(a)\equiv 0\pmod{l}$. 证毕.

由引理 18.6 知道前面描述的构造完全不需要考虑障碍问题. 事实上, 考虑 (18.25) 式中元素 $\prod_{i=1}^{e}c_i^{e_i}$, 由 (18.25) 式, 这是 V_l 中一个元素, 于是引理 18.6 告诉我们 $\mathrm{inv}_\wp(\prod c_i^{e_i})=0$, 但这只有当伴随在 $\mathbb{F}_{p^n}$ 中的元素是商 $\mathbb{F}_{p^n}^*/{\mathbb{F}_{p^n}^*}^l$ 中平凡元时才能发生, 从而 $\prod_{i=1}^{t}c_i^{e_i}$ 是一个 l 次幂. 进而在 $\mathbb{F}_{p^n}$ 中有

$$a^{k_a}b^{k_b}=x^l,\quad k_a=\sum e_ir_i,\ k_b=\sum e_is_i.$$

若 $k_b\neq 0\pmod{l}$, 就得出所求离散对数为 $-k_a/k_b\pmod{l}$.

由引理 18.6 知道, 若存在一个数域 K 满足基本假定, 则障碍问题是平凡的. 因此, 需要考虑如何保证这样的域的存在性.

对给定的数域 K 和模数 m, 射类群阶的计算已有很好的研究, 并且有很好的数论软件, 如 PARI, KANT 等来实现. 回顾射类群的定义:

$$1 \to U_m(K) \to U(K) \to (\mathcal{O}_K/m)^* \to Cl_m(K) \to Cl(K) \to 1.$$

由此正合列, 决定 $Cl_m(K)$ 的结构归结到决定 $U(K)$ 和 $Cl(K)$ 的结构, 以及使这些映射是有效可计算的. 更精确地说, 由于我们只关心 $Cl_m(K)$ 的阶, 因此只要计算 $Cl(K)$ 和 $U(K)/U_m(K)$ 的阶即可. $(\mathcal{O}_K/m)^*$ 的计算可忽略不计. 然而 $U_m(K)$ 在 $U(K)$ 中的指标的计算不是一件容易的事. 仅有的方法是应用有限 Abel 群中的一般算法, 该算法要求有关群由 Smith 正规形式给出. 特别地, 需要计算 K 中的一个基本单位系. 有关算法参见文献 [66]. 因此, 对于任意数域而言, 这个过程必须经过大量计算才能完全.

现在退一步来考虑这个问题. 对于一类特别的域, 考虑给出 $[U(K):U_m(K)]$ 的上界估计 (因而可给出射类域次数的下界估计).

若一个数域 K 的所有到 $\mathbb{C}$ 中的嵌入都是实嵌入, 则称 K 为全实的数域. 若其任意一个嵌入都不是实嵌入, 则称之为全虚的数域. 若全实数域中一个元素 α 的所有共轭均是负的, 则 α 称为全负的.

定义 18.12　*设 K 为一个数域, 若 K 是一个全实数域 K^+ 的全虚 2 次扩张, 则称 K 为一个 CM 域. 因此, 一个 CM 域可从一个全实数域 K^+, 加入 K^+ 中一个全负元素的平方根到 K^+ 而得到.*

分圆域 $K = \mathbb{Q}(\zeta_n)$ 是一个 CM 域 (令 $K^+ = \mathbb{Q}(\zeta_n^1 + \zeta_n^{-1})$ 为 K 的最大实子域, 则在 K^+ 中添入全负元 $\zeta_n^2 + \zeta_n^{-2} - 2$ 的平方根就得到 K).

定理 18.20　*设 K 是一个 CM 域, U 是其单位群, U^+ 是 K 的全实子域 K^+ 的单位群, W 是 K 中单位根群, 则*

$$[U : WU^+] = 1 \text{ 或 } 2.$$

证明　设 ϕ, ψ : $K \to \mathbb{C}$ 是两个嵌入. 对 $\alpha \in K$, 我们证明: $\phi^{-1}(\overline{\phi(\alpha)}) = \psi^{-1}(\overline{\psi(\alpha)})$. 由于 $\phi(K)/\phi(K^+)$ 是 2 次的, 故是一个正规扩张, $\phi(K^+)$ 被复共轭固定, 从而 $\phi(K) = \overline{\phi}(K)$. 特别地, $\phi^{-1}(\overline{\phi})$ 有意义. 现在考虑 $\phi^{-1}(\overline{\phi})$ 和 $\psi^{-1}(\overline{\psi})$. 两者均是 K 的自同构且均固定 K^+(因 K^+ 是全实的). 因而均属于 $\mathrm{Gal}(K/K^+)$. 但 K 是全虚的, 故两者均不能是恒等元, 从而它们必相等 (因 K/K^+ 是 2 次的).

因而存在 K 的一个自同构 $\lambda = \phi^{-1}(\overline{\phi})$, 它由共轭诱导出来, 且与 K 到 $\mathbb{C}$ 中的嵌入无关. 于是, 对 K 中一个元素 α, 记 $\overline{\alpha}$ 是 $\lambda(\alpha)$. 当然 $|\alpha|^2 = \alpha\overline{\alpha}$ 也无关于嵌入的

选择. 若 ε 是一个单位, 则 $\varepsilon/\bar{\varepsilon}$ 是一个绝对值为 1 的代数整数, 但这意味着 $\varepsilon/\bar{\varepsilon}$ 是一个单位根 (参见文献 [67], 引理 1.6).

可以定义映射 $\phi: U \to W$, $\phi(\varepsilon) = \varepsilon/\bar{\varepsilon}$. 考虑由 ϕ 诱导的映射 $\psi: U \to W/W^2$. 由于 W 是循环的, 有 $|W/W^2| = 2$. 下面计算 ψ 的核. 首先注意到, 对于一个全实单位 ε_1 和一个单位根 ζ, 令 $\varepsilon = \zeta\varepsilon_1$, 有

$$\phi(\varepsilon) = \phi(\zeta\varepsilon_1) = \zeta\varepsilon_1/\bar{\zeta}\varepsilon_1 = \zeta^2,$$

因此 $\varepsilon \in \ker(\psi)$. 反之, 若 $\phi(\varepsilon) = \zeta^2$, 考虑 $\varepsilon_1 = \zeta^{-1}\varepsilon$, 从 $\zeta^2 = \varepsilon/\bar{\varepsilon}$ 知 $\zeta^{-1}\varepsilon$ 必为实数, 因而 $\ker(\psi) = WU^+$, 从而 $[U : WU^+] \leqslant |W/W^2| = 2$. 更进一步, $[U : WU^+] = 2$ 当且仅当 $\phi(U) = W$, 而 $[U : WU^+] = 1$ 当且仅当 $\phi(U) = W^2$. 证毕.

推论 18.5 设 $K = \mathbb{Q}(\zeta_{p^n})$, 则 $[U : WU^+] = 1$.

证明 参见文献 [67] 推论 4.13.

下面将上述结果应用到指标 $[U : U_m]$ 的估计. 考虑 $m = \wp$ 的情形 ($\wp$ 为 K 的位于一个惰性有理素数 p 之上的素理想), 则 $u \in U_\wp$ 的条件是 $v_\wp(u-1) \geqslant 1$. 即 u 是主 $\wp$ 单位 $U_\wp^1$ 的一个元素, 或者说 $u \equiv 1 \pmod{\wp}$. 设 K 是 CM 域, 从而 WU_K^+ 在 U_K 中的指标为 1 或 2. Dirichlet 单位定理表明 U_K^+ 的自由部分由 $s = \frac{[K:\mathbb{Q}]}{2} - 1$ 个基本单位 $u_1, \cdots, u_s$ 生成, 加上 K 的单位根就组成 K 的整个单位群. 现在由 $U_\wp$ 的定义知道, 只要估计使得 $u_i^n \in U_\wp^1$ $(i = 1, \cdots,)$ 成立的指数 n 即可.

由于 p 是在 K 中惰性的, 故 p 在 K^+ 亦然. 令 $\wp_+ = \wp \cap K^+$. 由于 $u_i \in K^+$, 故 $u_i^{1+p+p^2+\cdots+p^s} \in U_{\wp_+}^1$. 由于 u_i 在 K^+ 中的整体范数为 1, 故 u_i 在有限域 $k_{\wp_+}$ 的像的范数也等于 1. 但是 $\wp|\wp_+$, 这表明 $u_i^{1+p+p^2+\cdots+p^s} \in U_\wp^1$ 或 $(u_i^{1+p+p^2+\cdots+p^s})^2 \in U_\wp^1$(取决于 WU_K^+ 在 U_K 中的指标). 设 ζ 是 W 中的一个非平凡元素, 则 $\zeta^{|W|} \equiv 1 \pmod{\wp}$, 因此我们得到

定理 18.21 *设 K 是一个次数为 n 的 CM 域, 令 $m = n/2$ 是其最大全实子域 K^+ 的次数. 设 p 是一个在 K 中惰性的有理素数, $\wp$ 是 K 中位于 p 上的素理想, 则有*

$$[U_K : U_{K,\wp}] \leqslant |W|[U_K : WU_K^+](1 + p + p^2 + \cdots + p^{m-1}).$$

于是我们可以给出射类域 $K_\wp/K$ 的次数估计:

推论 18.6 *我们有*

$$\frac{p^{2m}-1}{\operatorname{lcm}(|W|, [U_K : WU_K^+](1 + p + \cdots + p^{m-1}))} \Big| [K_\wp : K].$$

若假定 $(l, h(K)) = 1$ 且 $(l, |W(K)|) = 1$, m 为奇数, 则当 $l|(p^{m-1} - p^{m-2} + \cdots + 1)$ 时, 存在一个次数为 l 的扩张 L/K, 它正好在 $\wp$ 处分歧.

现在应用 CM 域来计算它的剩余类域中的离散对数. 设域 $k=\mathbb{F}_{p^n}$, 考虑 $\mathbb{F}_{p^n}^*$ 中一个子群的离散对数问题. 显然我们可以假定该子群不包含在 k 的真子域中, 因为否则我们的子群将落入一个更小的域, 这样将失去大域的安全性. 因而, 或者 n 为一个素数, 或者要研究多项式 x^n-1 在 $\mathbb{Z}$ 上的分解 (而第 2 种情形在 XTR 系统中就出现).

现在假设 $n=2m$, m 为奇数, 假设能够提升 k 到一个 CM 域 K, 且 p 在 K 中是惰性的, 于是要考虑 $x^{2m}-1$ 的分解. 首先, 有

$$\begin{aligned}x^{2m}-1&=(x^m+1)(x^m-1)\\&=(x-1)(x^{m-1}+x^{m-2}+\cdots+x+1)(x+1)(x^{m-1}-x^{m-2}+\cdots-x+1).\end{aligned}$$

设 l 为素数且 $l|p^{2m}-1$, 为了决定 $\mathbb{F}_{p^{2m}}^*$ 中 l 阶循环子群 C 是否包含在 $\mathbb{F}_{p^{2m}}$ 的一个真子域中, 必须分别考虑 $x^{2m}-1$ 的因子:

(a) $l\nmid p-1$, 否则 C 将包含于 $\mathbb{F}_p^*$ 中;

(b) $l\nmid p^{m-1}+\cdots+p+1$, 否则 $l|p^m-1$, 从而 C 包含于 $\mathbb{F}_{p^m}^*$ 中;

(c) $l\nmid p+1$, 否则 $l|p^2-1$, 从而 C 包含于 $\mathbb{F}_{p^2}^*$ 中;

因此, 我们有

引理 18.7 *设 C 是一个 l 阶循环子群, 则当 C 不包含于 $\mathbb{F}_{p^{2m}}$ 的真子域中时, 必有*

$$l|(p^{m-1}-p^{m-2}+\cdots+(-1)^{m-1}).$$

现在设 p 在 d 次 CM 域 $K/\mathbb{Q}$ 中是惰性的, C 是 $\mathbb{F}_{p^d}^*$ 中 l 阶子群, C 不包含于 $\mathbb{F}_{p^d}$ 的任何真子域中, 且 $(l,h(K))=(l,|W(K)|)=1$, 于是由推论 18.6, 存在一个 l 次扩张 L/K, 它恰在 $\wp|p$ 处分歧. 于是可以利用算法 18.3 来解 C 中的离散对数问题, 其中的障碍问题是平凡的. 因此, 从密码学角度来看, 最有趣的情形恰恰是我们能够应用 Brauer 群的情形. 总结起来, 就是下述:

定理 18.22 *设 K 是一个 $d=2m$ 次的 CM 域, p 是在 K 中惰性的有理素数, 则 $\mathbb{F}_{p^d}$ 中 l 阶循环子群 (l 满足推论18.6中条件) 中的离散对数可以利用算法18.3无障碍地解决, 其复杂度为 $L_{p^n}(1/2)$.*

证明 所有结论均由上面讨论可知, 而复杂度分析可参见 Adleman 和 Demarrais 的文章 [65].

为了将上述亚指数算法中的指数 1/2 进一步缩小, 则要利用数域筛法. 其基本思想是首先将 $\mathbb{F}_{p^n}$ 提升到一个固定的数域 F, 然后考虑 F 另一个扩张 K/F, 其次数 d 取决于 p 和 n. 如果适当选取次数 d 如下:

$$d=\left((3n)^{1/3}+o(1)\right)(\log p/\log\log p)^{1/3},$$

则光滑界 (从而因子基的大小尺度) 可降至

$$B=L_{p^n}(1/3,(8n/9)^{1/3}+o(1)).$$

特别地, 只要 $n < (\log p)^{1/2-\varepsilon}$(当 $p^n \to \infty$, $0 < \varepsilon = o(1)$), 则离散对数数域筛法的复杂度为 $L_{p^n}(1/3, (64/9)^{1/3} + o(1))$.

现在考虑 XTR 情形. 考虑 $\mathbb{F}_{p^6}$ 中一个 l 阶循环子群, $l|p^2-p+1$. 假定 K 是一个次数为 $6d$ (d 为奇数) 的 CM 域, 具有循环 Galois 群 $G = \langle\sigma\rangle$. 令 F 是被 σ^d 固定的 K 的子域, 则 $F/\mathbb{Q}$ 是一个 6 次的 CM 域 (参见文献 [68], 引理 18.2). 假定 p 在 $K/\mathbb{Q}$ 中是惰性的, 于是 p 在 $F/\mathbb{Q}$ 中亦然, 所以当 $(h(F), l) = 1$ 时, 在 F 中构造 l 次幂的障碍是平凡的. 由推论 18.6, 知 K 的在 $\beta|p$ 处分歧的射类域的次数被 $p^{3d}+1$ 整除, 但 d 是奇数表明 $p^3+1|p^{3d}+1$, 又 $(p^2-p+1)|p^3+1|p^{3d}+1$, 因此, 若 $(h(K), l) = 1$, 则存在 K 的一个次数 l 的扩张, 该扩张恰在 β 处分歧. 从而在 K 上的 l 次幂的构造的障碍也是平凡的. 总结上述讨论, 有

定理 18.23 设 $K/\mathbb{Q}$ 是一个次数为 $6n$(n 为奇数) 的Galois扩张, K 为 CM 域. 设 $F/\mathbb{Q}$ 是次数为 6 的 K 的 CM 子域. 假定 p 在 $K/\mathbb{Q}$ 中惰性且 $l|p^2-p+1$, $(h(K), l) = (h(F), l) = (|W(K)|, l) = 1$, 则在 F 和 K 中的 l 次幂的构造是无障碍的, 其中 $W(K)$ 记 K 中单位根的数目.

§18.6 函数域筛法

上节讨论了整体域中指标计算算法. 在该算法中应用 Brauer 群理论的主要困难是在一个数域 K 上的具有给定分歧和次数的扩张的存在性. 我们只能对 CM 域的情形得出一般结果. 而在函数域情形, 问题要简单得多. 主要原因是我们可以构造整体函数域, 其某些射类域的次数能够完全清晰地用公式给出.

设 K 是一个整体函数域, 其常数域为 $\mathbb{F}_q$. 设 $\wp$ 和 $\mathfrak{q}_0$ 是 K 的两个不同的位, 记 $K_\wp^{\mathfrak{q}_0}$ 是 K 的恰在 $\wp$ 处分歧的最大扩张, 且使得 $\mathfrak{q}_0$ 在 $K_\wp^{\mathfrak{q}_0}$ 中完全分裂. 则有 (参见文献 [69])

定理 18.24 $K_\wp^{\mathfrak{q}_0}$ 在 K 上的次数由下式给出:

$$[K_\wp^{\mathfrak{q}_0} : K] = h(K)\deg(\mathfrak{q}_0)\frac{q^{\deg(\wp)}-1}{q-1},$$

此处 $h(K)$ 记 K 的类数.

推论 18.7 设 $\deg(\mathfrak{q}_0) = 1$, $(h(K), l) = 1$, $l|\frac{q^{\deg(\wp)}-1}{q-1}$, 则存在一个 l 次扩张 L/K, 它恰在 $\wp$ 处分歧.

现在考虑一个位 $\wp$ 及素数 $l|\frac{q^{\deg(\wp)}-1}{q-1}$, 我们利用 K 的 Brauer 群来描述 $\mathbb{F}_{q^{\deg(\wp)}}$ 中 l 阶子群的离散对数问题. 为此, 充分应用整体函数域上循环代数理论与数域情形的完全类似性, 有关事实请参见文献 [70]. 在数域情形, 我们利用 Hasse-Brauer-Noether

定理和非分歧情形时不变量映射的清晰公式, 将离散对数问题转化成 Brauer 群的对应问题. 这些事实在整体函数域时也完全成立.

设 L/K 如上, $\mathfrak{q}$ 是一个非分歧素理想, 则循环代数 $A=(L/K,\sigma_{\mathfrak{q}},a)$ 的局部不变量由 $\mathrm{inv}_{\mathfrak{q}}(a)=\deg(\mathfrak{q})v_{\mathfrak{q}}(a) \pmod l$ 给出. 考虑局部扩张 $L_\wp/K_\wp$, 由 L/K 的定义, 它是分歧的. 由于 $[L_\wp:K_\wp]=l$ 且 $l|q^{\deg(\wp)}-1$, 它是一个 Kummer 扩张, 因此是可分的. 于是正如数域时一样, 有

$$\mathrm{Br}(L_\wp/K_\wp)\cong \mathbb{F}^*_{q^{\deg(\wp)}}/\mathbb{F}^{*l}_{q^{\deg(\wp)}}.$$

我们能够应用 Brauer 群 $\mathrm{Br}(L/K)$ 将分歧位 $\wp$ 处不变量与非分歧位处的不变量关联起来.

考虑 $R=\mathbb{F}_p[x]$ 和一个次数为 n 的不可约多项式 f, 于是 f 定义了 R 的分式域 $\mathbb{F}_p(x)$ 中一个 n 次的位 $\wp$, 有 $k_\wp\cong\mathbb{F}_{p^n}$. 设 S/R 是由 $H(x,y)=0$ 给出的一个扩张, 此处 H 是 R 上一个不可约的 d 次 (关于 y) 多项式. 定义 $K=\mathrm{Quot}(S)$, 假定 K 具有全常数域 $\mathbb{F}_p$, 也假定 $\wp$ 在 K 中完全分裂, 即 $\wp=\mathfrak{B}_1\cdots\mathfrak{B}_d$. 假定 y 在 $\mathcal{O}_\wp$ 上是整的, 则 $H(x,y)$ 可视为 $\mathcal{O}_\wp[y]$ 中一个元素. 假定 $H(x,y)$ 具有形式

$$H(x,y)=y^d+\sum_{i=0}^{d-1}y^ih_i(x),\quad h_i\in\mathcal{O}_\wp.$$

设 $\overline{h}_i$ 是 h_i 模 f 的约化, 从而 $\overline{H(x,y)}\in k_\wp[y]$, 此处

$$\overline{H(x,y)}=y^d+\sum_{i=0}^{d-1}y^i\overline{h}_i(x).$$

现在, $\wp$ 在 K 中完全分裂等价于 $\overline{H(x,y)}$ 分裂成 d 个线性因子 $y-\overline{\gamma}_i$, $\overline{\gamma}_i\in k_\wp$. 令 γ_i 是 $\overline{\gamma}_i$ 到 $\mathcal{O}_\wp$ 的一个提升, 则对于 $i=1,\cdots,d$, 存在 K 的位 $\mathfrak{B}_i$, 使得 $\mathfrak{B}_i|\wp$ 且 $(y-\gamma_i)\in\mathfrak{B}_i$. 更进一步, 此时, 剩余类域 $k_{\mathfrak{B}_i}=\mathcal{O}_{\mathfrak{B}_i}/\mathfrak{B}_i$ 同构于 $k_\wp[y]/(y-\overline{\gamma}_i)$ (这些结论的证明请参见文献 [57], III. 3.7).

下面讨论函数域筛法: 选取在 $\wp$ 之上的 d 个位中之一, 记为 $\mathfrak{B}$. 选取一个元素 $\gamma\in\mathcal{O}_\wp$, 使得 $(y-\gamma)\in\mathfrak{B}$, 现在搜寻互素多项式 $r,s\in\mathbb{F}_p[x]$, 使得 $ry+s$ 和 $r\gamma+s$ 是 B 光滑的 (此处, 若 $\mathbb{F}_p[x]$ 中一个元素可分解成次数小于 B 的不可约元素之积, 则称该元素是 B 光滑的, 若 $ry+s$ 在 $\mathbb{F}_p(x)$ 上的范是 B 光滑的, 则称 $ry+s$ 是 B 光滑的). 由于 γ 的选取, 知 $r\gamma+s$ 到 $k_\wp$ 的约化正好是 $ry+s$ 在 K 模 $\mathfrak{B}$ 的剩余类域中的像 (因为 $\wp$ 在 K 中分裂, $k_{\mathfrak{B}}$ 同构于 $k_\wp$).

选取 $l|\frac{p^n-1}{p-1}$, 由推论 18.7, 若 $(h(K),l)=1$, 则存在一个 l 次扩张 L/K, 它恰在 $\mathfrak{B}$ 处分歧. 定义两个因子基如下: S_1 包含所有次数不超过 B 的 $\mathbb{F}_p[x]$ 中不可约多项式. S_2 是从 S_1 获得的因子基, 它们是位于 S_1 的元素之上的 K 中所有素理想.

设 $ry+s$ 和 $r\gamma+s$ 是 B 光滑的, 其分解为

$$ry+s=\prod_{\mathfrak{D}\in S_2}\mathfrak{D}^{n_{\mathfrak{D}}},\quad r\gamma+s=\prod_{g\in S_1}g^{n_g}.$$

考虑由整体循环代数 $(L/K,\sigma,ry+s)$ 生成的关系, 它看上去如下:

$$\sum_{g\in S_1}h_g\mathrm{inv}_{\mathfrak{B}}(g)+\sum_{\mathfrak{D}\in S_2}\deg(\mathfrak{D})n_{\mathfrak{D}}f_{\mathfrak{D}}\equiv 0\pmod{l},$$

此处 $f_{\mathfrak{D}}$ 与数域情形相同, 它是 $\mathbb{Z}/l\mathbb{Z}$ 中元素, 使得 $\sigma^{f_{\mathfrak{D}}}=\sigma_{\mathfrak{D}}$, 此处 $\sigma_{\mathfrak{D}}$ 是 $\mathfrak{D}$ 处的 Frobenius.

只要收集到足够多这样的关系式, 就能够求解出 $\mathrm{inv}_{\mathfrak{B}}(g)$ 和 $f_{\mathfrak{D}}$. 而 $\mathrm{inv}_{\mathfrak{B}}(g)$, $g\in S_1$ 与 $k_{\wp}$ 中离散对数的关系如下: 由构造, 有 $k_{\mathfrak{B}}\cong k_{\wp}\cong\mathbb{F}_p[x]/(f)$, 因此 $\mathrm{inv}_{\mathfrak{B}}(g)$ 相关到 l 次单位根 $(g \bmod f)^{(p^n-1)/l}\in k_{\mathfrak{B}}^*/k_{\mathfrak{B}}^{*l}$ 的不变量. 我们首先计算充分多这样的不变量, 为了计算伴随到元素 $\alpha_1,\alpha_2\in\mathbb{F}_p[x]$ 的 l 次单位根的不变量, 我们搜寻随机指数 a_1,a_2, 使得

$$\alpha^{a_1}\alpha_2^{a_2}\equiv g_1g_2\cdots g_t\pmod{f},$$

其中 g_i 是 B 光滑的. 从两个这样的光滑关系, 我们就可以计算 $\mathrm{inv}_{\mathfrak{B}}(\alpha_1)$ 和 $\mathrm{inv}_{\mathfrak{B}}(\alpha_2)$, 从而得出所求离散对数问题的解.

因此我们从 Brauer 群理论导出了文献 [71] 中提出的函数域筛法. 特别地, 这表明只要小心选取相关参数, 该算法的期望复杂度为 $L_{p^n}(1/3)$. 下面就简要地说明一下如何获得该复杂度.

回顾上面提到的由多项式 $H(x,y)$ 给出的有理函数域的一个扩张. 设 $H(x,y)$ 的次数为 $d=\lceil c_1^{-1}n^{1/3}(\log n)^{-1/3}(\log p)^{1/3}\rceil$, 此处 c_1 为一待定常数. 假定有 $H(x,\gamma)\equiv 0\pmod{f}$, 此处 γ 的次数为 $d'=\lceil n/d\rceil$. 选取 $r,s\in\mathbb{F}_p[x]$, 其次数不超过 $c_2n^{1/3}$ $(\log n)^{2/3}$ $(\log p)^{-2/3}$, 此处 c_2 为一待定常数. 由对 γ 的假定, 知 $r\gamma+s$ 的次数不超过

$$(c_1+o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3}.$$

其次, $ry+s$ 的范为 $r^dH(x,-s/r)$, 故其次数不超过

$$(c_2/c_1+o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3}.$$

因此 $(r\gamma+s)N(ry+s)$ 的次数不超过

$$D=\lceil(c_1+c_2/c_1+o(1))n^{2/3}(\log n)^{1/3}(\log p)^{-1/3}\rceil.$$

假定：若 r 和 s 是随机选取的，则多项式 $(r\gamma+s)N(ry+s)$ 也是随机分布的 (其次数不超过 D).

令 $Q=p^D$，而置光滑性界为 $b=\log_p(L_Q(1/2,1/\sqrt{2}))$，则一个对 (r,s) 是 b 光滑的概率至少为

$$L_Q(1/2,-1/\sqrt{2}+o(1)),$$

此处必须假定 $\log p<n^{1/2-\varepsilon}$ $(0<\varepsilon=o(1)$，参见前面提到的 Adleman 和 Huang 的文章[71]). 因子基中元素个数界于 $L_Q(1/2,1/\sqrt{2})$，故要检验 $L_Q(1/2,\sqrt{2}+o(1))$ 个对 (r,s). 由于存在

$$p^{2c_2n^{1/3}(\log n)^{2/3}(\log p)^{-2/3}}$$

个适合者，从而

$$L_Q(1/2,\sqrt{2})\leqslant p^{2c_2n^{1/3}(\log n)^{2/3}(\log p)^{-2/3}},$$

于是得出不等式

$$\frac{c_2+c_1^2}{3c_1}\leqslant c_2^2,$$

从而有 $c_1=(2/3)^{1/3}$, $c_2=(3/9)^{1/3}$，故

$$\begin{aligned}D&=\big(2(2/3)^{1/3}+o(1)\big)n^{2/3}(\log n)^{1/3}(\log p)^{-1/3},\\ b&=L_{p^n}[1/3,(4/9)^{1/3}+o(1)].\end{aligned}$$

从光滑对 (r,s) 获得的关系形成一个模 l 的稀疏线性方程组，解此方程组的复杂度是

$$L_{p^n}[1/3,(32/9)^{1/3}+o(1)].$$

最后，我们必须将给定的元素 α_1 和 α_2 相关到因子基中元素. 为此，要考虑一个随机选取的次数不超过 n 的多项式 $g\in\mathbb{F}_p[x]$ 是 B 光滑的概率. 可以证明：若 $p^6<n$，则此步骤的复杂度由 $L_{p^n}[1/3,(3/2)^{1/3}]$ 给出，于是可知总的算法复杂度是 $L_{p^n}[1/3]$.

§18.7 (超) 椭圆曲线离散对数, Tate 对和 Brauer 群

在前面各节中，我们讨论了有限域上离散对数问题与 Brauer 群之间的关系. 现在，我们将探讨椭圆曲线离散对数问题与 Brauer 群之间的联系.

我们回顾 15.6 节中的有关内容. 有以下结果：

定理 18.25 设 $E/\mathbb{F}_q$ 是一条椭圆曲线，l 为素数，$l|q-1$(因而 $\mathbb{F}_q$ 包含 l 次单位根群 μ_l)，则存在一个非退化对

$$\phi_l:\quad E(\mathbb{F}_q)[l]\times E(\mathbb{F}_q)/lE(\mathbb{F}_q)\to\mu_l.$$

定理 18.25 中的 ϕ_l 称为 Tate-Lichtenbaum 对, 它的值可如下计算: 设 $P \in E(\mathbb{F}_q)[l]$, $Q \in E(\mathbb{F}_q)$, 选取除子 D_P 和 D_Q, 使得 D_P 和 D_Q 分别在 $(P)-(\mathcal{O})$ 和 $(Q)-(\mathcal{O})$ 的除子类中, 且 D_P 和 D_Q 互素. 由于 $lP=\mathcal{O}_E$, 故 lD_P 是一个函数 f_{D_P} 的除子. 于是 ϕ_l 的值如下:

$$\phi_l(P,Q) = (f_{D_P}(D_Q))^{(q-1)/l} \in \mu_l(\mathbb{F}_q). \tag{18.28}$$

给定 P 和 Q, 设 $Q=nP$, 选取一个点 $\widetilde{P}$, 满足 $\phi_l(P,\widetilde{P})=\zeta_0 \in \mu_l$, $\zeta_0 \neq 1$. 计算 $\phi_l(Q,\widetilde{P})=\zeta_1$. 因为 ϕ_l 是非退化的, 有 $\zeta_l=\zeta_0^n$, 因此, 在 $\mathbb{F}_q$ 中的离散对数问题的解就给出在椭圆曲线 E 上的离散对数问题的解.

(18.28) 式直接在有限域上给出了 ϕ_l 的定义, 然而, Frey 和 Rück 指出, 我们也能够从局部域上 Abel 簇的对偶理论得出它. 下面我们来回顾这个方法, 并表明该方法是如何将它与 Brauer 群的算术理论联系起来的.

首先, 将 $E/\mathbb{F}_q$ 提升为定义在 $\mathbb{Q}_p$ 的一个扩张 K 上的一条适当的椭圆曲线 E. 令 $\overline{K}$ 是 K 的代数闭包, G_K 是 K 的绝对 Galois 群, 则有 Tate 对

$$H^1(G_K, E(\overline{K}))[l] \times E(K)/lE(K) \to H^2(G_K, \overline{K}^*)[l] \cong \mathbb{Z}/l\mathbb{Z}. \tag{18.29}$$

对于上述 Tate 对的定义, 可参见文献 [72]. 下面将考察 Tate 对和 Tate-Lichtenbaum 对 ϕ_l 之间的关系. 为此, 我们描述 Tate 对在 Brauer 群中的像.

考察两个正合序列

$$0 \longrightarrow H(E) \longrightarrow \mathrm{Div}_0(E) \longrightarrow \mathrm{Pic}_0(E) \longrightarrow 0, \tag{18.30}$$

和

$$0 \longrightarrow K^* \longrightarrow \overline{K}(E) \longrightarrow H(E) \longrightarrow 0, \tag{18.31}$$

此处, $H(E)$ 记主除子群, $\mathrm{Div}_0(E)$ 记 $E/\overline{K}$ 上零次除子的 G_K 模, 而 $\mathrm{Pic}_0(E)=\mathrm{Div}_0(E)/H(E)$ 是 E 的 Picard 群, $\overline{K}(E)$ 记 $E/\overline{K}$ 的函数域. 由于 E 具有 K 有理点, 故有 $H^1(G_K,\mathrm{Div}_0(E))=0$, 从而正合序列 (18.30) 产生下述正合列:

$$\begin{aligned}\cdots \longrightarrow 0 = H^1(G_K,\mathrm{Div}_0(E)) &\longrightarrow H^1(G_K, E(\overline{K}))\\ &\xrightarrow{\ \delta\ } H^2(G_K, H(E)),\end{aligned} \tag{18.32}$$

而正合序列 (18.31) 给出另一个长正合列

$$\begin{aligned}\cdots \longrightarrow H^2(G_K,\overline{K}(E)^*) &\xrightarrow{\ \phi\ } H^2(G_K, H(E))\\ &\longrightarrow H^3(G_K,K^*)=0,\end{aligned} \tag{18.33}$$

此处, 用到了 K 是上同调维数 2 这个事实, 从而 $H^3(G_K, K^*) = 0$. 设 $f_\sigma \in H^1(G_K, E(\overline{K}))_l$, 为了计算 $\delta(f_\sigma)$, 选取 f_σ 到 $\mathrm{Div}_0(E)$ 的一个提升 $\widehat{f_\sigma}$, 则有

$$f_{\sigma,\tau} = (\delta f)_{\sigma,\tau} = \widehat{f}_\tau^\sigma - \widehat{f}_{\sigma\tau} + \widehat{f}_\sigma, \tag{18.34}$$

这是 $H^2(G_K, H(E))$ 中一个元素.

由 (18.33) 式, 映射 ϕ 是满的, 故存在元素 $\beta \in H^2(G_K, \overline{K}(E)^*)$, 使得 $\phi(\beta) = \delta(f_\sigma)$. 令 D_Q ($\in \mathrm{Div}_0(E)$) 位于 $(Q) - (\mathcal{O}_E)$ 所在除子类中, 而 $f_{\sigma,\tau}$ 是 β 所在类中的一个 2 上闭链. 若 $(f_{\sigma,\tau})$ 的支集和 D_Q 是互素的, 则可以定义

$$c_{\sigma,\tau} = f_{\sigma,\tau}(D_Q) = \prod_{S\in E} f_{\sigma,\tau}(S)^{n_S},\ D_Q = \sum n_S S, \tag{18.35}$$

这是取值在 $\overline{K}^*$ 中的一个 2 上闭链, 从而定义了 $H^2(G_K, \overline{K}^*)$ 中一个类 $[c_{\sigma,\tau}]$, 但 $H^2(G_K, \overline{K}^*)$ 同构于 K 的 Brauer 群, 从而 $[c_{\sigma,\tau}]$ 可视为 K 的 Brauer 群中之一元. 而 Lichtenbaum 在其重要论文 [32] 中证明了 β 总包含一个 2 上闭链与 D_Q 互素. 于是我们得出下述对:

$$\begin{array}{llll} \langle\,,\rangle: & H^1(G_K, E(\overline{K}))_l \times E(K)/lE(K) & \longrightarrow & H^2(G_K, \overline{K}^*), \\ & f_\sigma \times D_P & \longmapsto & \langle f_\sigma, D_P\rangle = [c_{\sigma,\tau}]. \end{array} \tag{18.36}$$

Lichtenbaum 在上面引述的文章中证明了这个对就是 Tate 原来所定义的对 (18.29) (至多差一个正负符号). 特别地, 它是非退化和双线性的, 而且 (18.36) 式给出的对可以有效的计算其值. 这是因为下述的:

引理 18.8 设 K 包含 l 次单位根, 令 π 是 K 的一素元, 而 $\langle\tau\rangle$ 是分歧扩张 $K(\pi^{1/l})/K$ 的Galois群. 假设 l 不等于 K 的特征且 E 模 π_K 具有好的约化, 则有

$$H^1(G_K, E(\overline{K}))_l = \mathrm{Hom}(\langle\tau\rangle, E(K)_l). \tag{18.37}$$

证明 设 K_u/K 是 K 的最大非分歧扩张. 因为 l 不等于 $\overline{K}$ 的特征且 E 有好的约化, 故

$$H^1(\mathrm{Gal}(K_u/K), E(K_u))_l = H^2(\mathrm{Gal}(K_u/K), E(K_u)) = 0. \tag{18.38}$$

而关于子群 $H = \mathrm{Gal}(\overline{K}/K_u) \subset \mathrm{Gal}(\overline{K}/K)$ 的扩张 - 限制序列 (inflation-restriction sequence) 给出

$$\begin{aligned} 0 \longrightarrow\ & H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K}))^{\mathrm{Gal}(K_u/K)} \xrightarrow{\ \mathrm{inf}\ } H^1(G_K, E(\overline{K})) \\ \xrightarrow{\ \mathrm{res}\ }\ & H^1(\mathrm{Gal}(K_u/K), E(\overline{K}))^{\mathrm{Gal}(\overline{K}/K_u)} = 0, \end{aligned}$$

因此有

$$H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K}))_l^{\mathrm{Gal}(K_u/K)} = H^1(G_K, E(\overline{K}))_l. \tag{18.39}$$

而下述 $G/H = \mathrm{Gal}(\overline{K}/K_u)$ 模的正合序列

$$0 \longrightarrow E(\overline{K})_l \longrightarrow E(\overline{K}) \xrightarrow{l} E(\overline{K}) \longrightarrow 0$$

给出下述长正合列:

$$\begin{aligned} \cdots \longrightarrow \quad & E(K_u) \quad \xrightarrow{l} \quad E(K_u) \\ \longrightarrow\ & H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K}))_l \longrightarrow H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K})) \\ \xrightarrow{l}\ & H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K})) \longrightarrow \quad \cdots, \end{aligned}$$

因此

$$\begin{aligned} E(K_u)/lE(K_u) &\longrightarrow H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K})_l) \\ &\longrightarrow H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K}))_l \longrightarrow 0. \end{aligned}$$

但注意到 $l \neq \mathrm{char}(\overline{K})$ 且 E 有好的约化, 从而 $E(K_u)$ 是 l 可除的, 于是 $E(K_u)/lE(K_u) = 0$. 将这些与 (18.39) 式结合, 就有

$$H^1(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K}))_l = \mathrm{Hom}(\mathrm{Gal}(\overline{K}/K_u), E(\overline{K})_l)^{\mathrm{Gal}(K_u/K)},$$

此处用到了以下事实: 由于 E 具有好的约化, 由 Neron-Ogg-shafarevich 判别法则, $\mathrm{Gal}(\overline{K}/K)$ 在 $E(\overline{K})$ 上的作用是非分歧的, 从而 $\mathrm{Gal}(\overline{K}/K_u)$ 在 $E(\overline{K})_l$ 上的作用是平凡的.

$\mathrm{Hom}(G_{K_u}, E(\overline{K})_l)$ 的每一个元素都在 G_{K_u} 的最大 l 商上分解, 而这个商由 $\mathrm{Gal}(K_u(\pi^{1/l})/K_u) = \langle\tau\rangle$ 给出. 又由于 τ 与 $\mathrm{Gal}(K_u/K)$ 的所有元素可交换, 于是我们获得 (18.37) 式中的结果, 引理证毕.

设 f_τ 是 $H^1(G_K, E(\overline{K}))_l$ 中一个元素, 由引理 18.8, f_τ 由 $\tau \to P$, $P \in E(K)_l$ 所给出. 此时, 伴随的 2 上闭链 $(\delta f)_{\tau^i,\tau^j}$ 具有非常特殊的形式: 按照

$$\widehat{f}_{\tau^i} = (i - d*l)(P) - (i - d*l)(\mathcal{O}), \quad i = d*l + r,\ r < l,$$

将 f_τ 提升到 $\mathrm{Div}_0(E)$, 于是按 (18.34) 式进行, 有

$$\begin{aligned} \delta f_{\tau^i,\tau^j} &= i(P) - i(\mathcal{O}) - ((i+j)(P) - (i+j)(\mathcal{O})) + j(P) - j(\mathcal{O}) \\ &= 0, \qquad \text{若}\, i + j < l, \\ \delta f_{\tau^i,\tau^j} &= i(P) - i(\mathcal{O}) - ((i+j-l)(P) - (i+j-l)(\mathcal{O})) + j(P) - j(\mathcal{O}) \\ &= l(P) - l(\mathcal{O}), \qquad \text{若}\, i + j \geqslant l, \end{aligned}$$

因此, 有

$$(\delta f)_{\tau^i,\tau^j} = \begin{cases} 0, & 若\ i+j<l, \\ l(P)-l(\mathcal{O}), & 若\ i+j \geqslant l. \end{cases}$$

因为 $lP = \mathcal{O}$, 故知道 $l(P) - l(\mathcal{O})$ 是伴随到一个函数 f_P 的主除子. 因此 Tate-Lichtenbaum 对在 $H^2(G_K, \overline{K}^*)$ 中的像由 2 上闭链

$$(\delta f)_{\tau^i,\tau^j}(D_Q) = \begin{cases} 1, & 若\ i+j<l, \\ f_P(D_Q), & 若\ i+j \geqslant l \end{cases}$$

所在的类给出. 注意, $f_P(D_Q)$ 的值必须考虑是在

$$K^*/N_{L/K}(L^*) \cong k^*/k^{*l} \cong \mu_l(k)$$

中的. 事实上, Frey 和 Rück[31] 证明了: 通过提升到局部域再约化到有限域所获得的 Tate-Lichtenbaum 对的值, 和定义在有限域上的 Tate-Lichtenbaum 对的值是一样的. 因此, 我们通过计算有限域上 Tate-Lichtenbaum 对的值, 就可得到描述 Brauer 群中元素的上述 2 上闭链.

因此, 借助于 Brauer 群来描述 Tate 对又一次导致定义在局部域上分歧扩张的 2 上闭链的研究. 这和我们在前几节中讨论有限域上离散对数问题的方法是完全一样的. 正如我们在前几节所看到的, 这就导出解离散对数问题的熟知方法 —— 指标计算.

以上的方法实际上可以推广到任意代数曲线情形, 而不必限制在椭圆曲线时. 这就是 Frey 和 Rück 的上述提到的论文的主要内容. 下面我们简单地总结一下 Frey 和 Rück 的结果.

我们开始于一般的情形, 设 K 是一个域, 其绝对 Galois 群记为 G_K, 而 A 是定义在 K 上的一个主极化 Abel 簇, p 为一素数且 $p \neq \mathrm{char}(K)$. 令 K_S 记 K 的可分闭包, 将其视为一个 G_K 模. 而 μ_p 是 K_S 中 p 次单位根群. 于是有 G_K 模的正合序列 (Kummer 序列)

$$0 \longrightarrow A(K_s)[p] \longrightarrow A(K_s) \xrightarrow{p} A(K_S) \longrightarrow 0.$$

应用 Galois 上同调, 得出正合序列

$$0 \longrightarrow A(K)/pA(K) \xrightarrow{\delta} H^1(G_K, A(K_S)[p]) \xrightarrow{\alpha} H^1(G_K, A(K_S))[p] \longrightarrow 0.$$

由于 A 是主极化的, 故作为 G_K 模, $A(K_S)[p]$ 是自对偶的, 因此应用 Cup 积, 得到 Tate 对

$$\begin{aligned}\langle\,,\rangle: \quad A(K)/pA(K)\times H^1(G_K,A(K_S))[p] &\longrightarrow H^2(G_K,\mu_p)\\ \langle P+pA(K),\gamma\rangle_K &\longmapsto \delta(P+pA(K))\cup\alpha^{-1}(\gamma).\end{aligned} \tag{18.40}$$

群 $H^2(G_K,\mu_p)$ 是一个对 K 的算术十分重要的群, 它同构于 $H^2(G_K,K_S^*)[p]$, 但 $H^2(G_K,K_S^*)$ 是 K 的 Brauer 群, 于是 $H^2(G_K,K_S^*)[p]$ 由 K 的 Brauer 群 $\mathrm{Br}(K)$ 中阶除尽 p 的元素组成. 而我们能够从上述 Tate 对得到的信息, 取决于由 Brauer 群和对的非退化性给出的信息. 例如, 当 K 是一个有限域时, $\mathrm{Br}(K)=\{0\}$, 我们得不到有趣的东西. 但当 K 是一个 l-adic 域, 其剩余类域为有限域时, 情形就不同了.

定理 18.26 (Tate) *设 K 是一个 l-adic域, 其剩余类域为有限域 k, 则 $\langle\,,\rangle_K$ 是非退化的.*

因此, 对于 l-aic 域上的主极化 Abel 簇, 已经将 $A(K)[p]$ 中的离散对数问题转化成 $\mathrm{Br}(K)[p]$ 中对应的问题 (只要能够在多项式时间内计算对 $\langle\,,\rangle_K$ 的值).

假定 K 包含 p 次单位根 ζ_p, 即 $p|q-1$, 此处 q 是 K 的剩余类域的势. 与引理 18.8 的证明类似, 我们可以证明下述:

引理 18.9 *设 K 包含 p 次单位根 ζ_p, 令 L_p 是 K 的次数为 p 的分歧扩张, 则*

$$H^1(G_K,A(K_S))[p]=\mathrm{Hom}(\mathrm{Gal}(L_p/K),A(K)[p]).$$

结合 (18.40) 式, 定理 18.26 和引理 18.9, 就有

推论 18.8 *设 K 包含 p 次单位根 ζ_p, 令 L_p 是 K 的 p 次分歧扩张, 则存在由 Tate 对诱导出的非退化对 $\langle\,,\rangle$:*

$$\langle\,,\rangle: \quad A(K)/pA(K)\times\mathrm{Hom}(\mathrm{Gal}(L_p/K),A(K)[p])\to\mathrm{Br}(K)[p].$$

假定 k 是一个阶为 $q=l^f$ 的有限域, p 是一个整除 $q-1$ 的素数. 设 C 是定义在 k 上的一条射影曲线, 而 A 是其 Jacobian. 将 (C,A) 提升到 l-adic 域 K 上的 $(\widetilde{C},\widetilde{A})$, K 的剩余类域为 k, 并应用推论 18.8 到 $\widetilde{A}$. 注意到有关 K 的 Brauer 群的知识, 就有

定理 18.27 *设 τ 是 $\mathrm{Gal}(L_p/K)$ 的一个生成元, 而 P_1 和 P_2 是 $\widetilde{A}(K)$ 中两个点, P_2 的阶为 p. 设 ϕ 是从 $\mathrm{Gal}(L_p/K)$ 到 $\widetilde{A}(K)[p]$ 的同态, 它将 τ 映到 P_2. 用除子类群中互素的除子 D_i 表示 P_i-P_0, 而设 f_2 是 $\widetilde{C}$ 上一个函数, 其除子为 $p\cdot D_2$, 则*

$$\langle P_1+p\widetilde{A}(K),\phi\rangle=f_2(D_1)N_{L_p/K}(L^*).$$

注意到 $\widetilde{A}(K)[p]$ 同构于 $A(k)[p]$, $\widetilde{A}(K)/p\widetilde{A}(K)$ 同构于 $A(k)/pA(k)$, 并且 $K^*/N_{L_p/K}(L_p^*)$ 同构于 k^*/k^{*p}, 有

定理 18.28　*存在着一个非退化对 $\langle\,,\rangle_k$:*

$$\langle\,,\rangle:\quad A(k)/pA(k)\times A(k)[p]\longrightarrow k^*/k^{*p},$$

其计算法则如下: 设 P_1 和 P_2 是 $A(k)$ 中的点, P_2 的阶为 p, 用除子类群中互素的除子 D_i 表示 P_i-P_0, 而令 f_2 是 C 上的函数, 其除子为 pD_2, 则

$$\langle P_1+pA(k),P_2\rangle=f_2(D_1)\cdot k^*/k^{*p}.$$

由定理 18.28 知道: 如果能够快速有效地计算 $f_2(D_1)$, 则可以将 $J_C(k)[p]$ 中的离散对数问题转化为与 k 相关的一个群中的离散对数问题. 但注意到我们结束于 k 的乘法群之中, 而在这个群中, 有已知的亚指数时间攻击方法 —— 指标攻击 —— 我们在前几节详细讨论过的事实.

于是, 问题归结到如何有效快速计算 $f_2(D_1)$, 或者说是下述问题: 设 k 是一个特征不整除 m 的有限域, 设 X 是定义在 k 上的一条亏格为 g 的射影不可约非奇异曲线. 对于元素 $\overline{D}\in\mathrm{Pic}_0(X)[m]$ 和 $\overline{E}\in\mathrm{Pic}_0(X)$, 取任意除子 $D\in\overline{D}$ 并找出 X 上一个函数 f, 使得其除子等于 mD; 取一个除子 $E\in\overline{E}$ (它与 D 互素), 然后计算 $f(E)$.

下面给出一个算法解决上述问题, 该算法计算一个 $f(E)$ 的复杂度是 $O(\log m)$ 个初等运算. 此处, 所谓一个初等运算, 指的是下述的计算:

(*) 设 A_1 和 A_2 是两个次数为 g 的正除子; 找出一个次数为 g 的正除子 A_3 和一个函数 h, 使得 h 的除子等于 $A_1+A_2-A_3-gP_0$, 此处假定 P_0 是 X 上的一个固定的 k 有理点 (假定 P_0 的存在性).

上述条件事实上表明在 $\mathrm{Pic}_0(X)$ 中的群运算可以清晰的进行计算. 下面我们来解释这一点:

设 k 上的亏格 g 的射影不可约非奇异曲线有一个 k 有理点 P_0, 则 Riemann-Roch 定理断言, $\mathrm{Pic}_0(X)$ 中每一个类都包含一个形如 $A-gP_0$ 的除子, 其中 A 是 X 上次数为 g 的正除子, 事实上, 设 $D\in\mathrm{Div}_0(X)$, 由 Riemann-Roch 定理, 有

$$l(D+gP_0)-l(\mathfrak{K}_X-D-gP_0)=\deg(D+gP_0)-g+1=1,$$

其中 $\mathfrak{K}_X$ 是 X 的典范除子. 于是存在 $f\in\mathscr{C}(D+gP_0)$, 从而 $\mathrm{div}(f)\geqslant -D-gP_0$, 但 $\deg(\mathrm{div}(f))=0$, 故存在某个次数为 g 的除子 A, 使得 $\mathrm{div}(f)=-D-gP_0+A$. 易知 A 必为正除子, 从而 $D\sim A-gP_0$. 可见 $\mathrm{Pic}_0(X)$ 中每一个类均包含一个形如 $A-gP_0$ 的除子. 假设知道满射 $C_g: A\to\overline{A-gP_0}\in\mathrm{Pic}_0(X)$ (A 为任意次数为 g 的正除子), 它将每一个次数为 g 的正除子映射到 $A-gP_0$ 所在的除子类, 于是条件 (*) 表明 $\mathrm{Pic}_0(X)$ 中的加法是清晰中计算的.

需要注意的是, 一般而言, 关于条件 (*) 和映射 C_g 这两个假定是不易满足的. 但是, 在下述两种情形下, $\mathrm{Pic}_0(X)$ 中的计算问题的解答是熟知的:

例 18.3 若 X 是由仿射方程 $y^2 = x^3 + ax + b$ 给出的椭圆曲线, P_0 是无穷远点, 则 3 个点 $P_i = (x_i, y_i)$ $(i = 1,2,3)$ 满足 $\overline{P_1 - P_0} + \overline{P_2 - P_0} + \overline{P_3 - P_0} = 0$(在 $\mathrm{Pic}_0(X)$ 中成立) 当且仅当点 (x_i, y_i) $(i = 1,2,3)$ 位于直线 $l(x,y)$ 上, 更进一步, $\overline{P_1 - P_0}$ 是 $\overline{P_2 - P_0}$ 的逆当且仅当 $x_1 = x_2$ 且 $y_1 = -y_2$, 因此条件 (*) 中的函数 h 由方程 $l(x,y)/(x - x_3)$ 给出.

例 18.4 设 X 是 k 上一条超椭圆曲线, 则加法律 (*) 可由一个约化算法给出 (例如, 参见本书第十六章, 或文献 [46 ~ 48]). 现在设 D 是一个除子, 使得 $\overline{D} \in \mathrm{Pic}_0(X)[m]$, 而 $E = \sum_{i=1}^{r} a_i P_i \in \mathrm{Div}_0(X)$, D 和 E 无公共点 (即 D 和 E 互素), 由于 $m\overline{D} = 0$, 故 mD 为主除子, 从而存在函数 f, 使得 $\mathrm{div}(f) = mD$. 于是定义 $f(E) = \prod_{i=1}^{r} f(P_i)^{a_i}$.

设 E 的支集不含有 P_0, 而 S 是 $\mathrm{Pic}_0(X)$ 的有限子群, 假定 S 具有一个代表元集合 $\{A_S\}$, 使得所有 $A_S - gP_0$ 与 E 互素. 我们固定这样一个代表元集并定义 $S \times k^*$ 上的群律

$$(s_1, a_1) \odot (s_2, a_2) = (C_g(A_{S_3}), a_1 a_2 h(E)),$$

此处 A_{S_3} 和 h 分别是对应于 A_{S_1} 和 A_{S_2} 的步骤 (*) 中的除子和函数, 即有

$$A_{S_1} + A_{S_2} - A_{S_3} - gP_0 = \mathrm{div}(h).$$

显然 S_3 是 S_1 与 S_2 在 S 中的和, 而关于 A_S 和 E 的假定保证了 $h(E)$ 是 k 中非零元素.

引理 18.10 设 $E \in \mathrm{Div}_0(X)$ 与 P_0 互素, $\overline{D} \in \mathrm{Pic}_0(X)[m]$, 假设 $\mathrm{Pic}_0(X)$ 中由 $\overline{D}$ 生成的子群具有一个与 E 互素的代表元集合, $\mathcal{O}$ 的代表元设为 gP_0, 则

$$\underbrace{(\overline{D}, 1) \odot (\overline{D}, 1) \cdots \odot (\overline{D}, 1)}_{m\text{个}} = (0, f(E)),$$

此处 f 是 X 上的函数, 其除子等于 mD.

证明 设 A_i 是 $i\overline{D}$ 的代表元, A_i 与 E 互素, 则立即可知

$$\underbrace{(\overline{D}, 1) \odot (\overline{D}, 1) \cdots \odot (\overline{D}, 1)}_{i\text{个}} = (i\overline{D}, h_i(E)),$$

此处, h_i 的除子为 $iA_1 - A_i - (i-1)gP_0$. 由于 $m\overline{D} = \mathcal{O}$, 故 $A_m = gP_0$ (因有 $\mathcal{O}$ 的代表元为 gP_0), 从而 h_m 的除子为 $mA_1 - A_m - (m-1)gP_0 = m(A_1 - gP_0) = mD$, 可见 $h_m(E) = f(E)$. 证毕.

借助于引理 18.10, 我们能够在 $O(\log m)$ 个初等运算内计算出 $f(E)$ (在群 $(\langle\overline{D}\rangle\times k^*,\odot)$ 中应用重复平方-加算法).

注记 18.2　若 $g=1$, 则可以应用引理 18.10 计算椭圆曲线的 Weil 对.

注记 18.3　设 $\overline{D}\in\mathrm{Pic}_0(X)[m]$ 且 $\overline{E}\in\mathrm{Pic}_0(X)$, 为了应用引理 18.10 计算 $f(E)$, 并不必假定除子 $E\in\overline{E}$ 与每一个 $i\overline{D}$ 的代表元互素, 而只有那些 (在重复平方 - 加算法中) 用来完成加法的代表元是重要的, 因此 E 能够在 $O(\log m)$ 步之内选出.

定理 18.29　*设 $\overline{D}\in\mathrm{Pic}_0(X)[m]$, $\overline{E}\in\mathrm{Pic}_0(X)$, 取除子 $D\in\overline{D}$ 和 $E\in\overline{E}$, 使得 D 和 E 互素, 设 f 是一个除子为 mD 的函数, 则 $f(E)$ $(\mathrm{mod}\ k^{*m})$ 可在 $O(\log m)$ 个初等运算 $(*)$ 内算出.*

注记 18.4　一般而言, 条件 K (因而其剩余类域 $k=\mathbb{F}_q$) 包含 p 次单位根和 $J_X(k)$ 具有密码学兴趣的 p 阶 k 有理点并不能够同时得到满足. 对于椭圆曲线而言, 我们可以给出更精确的叙述如下：

定理 18.30　*设 E 是定义在 $\mathbb{F}_q$ 上的一条椭圆曲线, p 为一个素数, π 是 $\mathbb{F}_q$ 上的Frobenius自同构在 E 上诱导出的自同构, 则 $\mathbb{Z}/p\mathbb{Z}$ 能够嵌入 $E(\mathbb{F}_{q^f})$ (即 $E(\mathbb{F}_{q^f})$ 中有 p 阶 $\mathbb{F}_{q^f}$ 有理点) 当且仅当 π^f 的迹同余于 q^f+1 $(\mathrm{mod}\ p)$, 而此时在 $E(\mathbb{F}_{q^f})$ 的 p 阶子群中对应的离散对数问题可以约化为有限域 $\mathbb{F}_{q^{fm}}$ 中单位群 μ_p 的离散对数问题, 此处 m 是使得 π^{fm} 的迹模 p 同余于 2 的最小正整数 m.*

证明　第 1 部分结论可由椭圆曲线上有理点个数与迹的关系立得. 又若 m 如定理 18.30 中, 则由

$$\mathbb{Z}/p\mathbb{Z}\hookrightarrow E(\mathbb{F}_{q^f})\subset E(\mathbb{F}_{q^{fm}})$$

及

$$\#E(\mathbb{F}_{q^f})=q^f+1-\mathrm{tr}(\pi^f),\quad \#E(\mathbb{F}_{q^{fm}})=q^{fm}+1-\mathrm{tr}(\pi^{fm})$$

知

$$p|q^f+1-\mathrm{tr}(\pi^f)|q^{fm}+1-\mathrm{tr}(\pi^{fm}),$$

但是

$$\mathrm{tr}(\pi^{fm})\equiv 2\pmod p,$$

故

$$q^{fm}-1\equiv 0\pmod p,$$

即 $p|q^{fm}-1$.

对 $k=\mathbb{F}_{q^{fm}}$ 应用定理 18.28 (或定理 18.25), 就得出定理 18.30 的第 2 部分结论, 证毕.

从现在开始, 我们将给出 Tate 对在某些密码学问题中的应用. 首先给出几个概念. 设 G 是一加法群, 不妨设 G 的阶为素数.

(a) DLP (离散对数问题) 是指: 给定两个群元素 g 和 $h \in G$, 找出整数 n, 使得 $h = ng$;

(b) DHP (Diffie-Hellman 问题) 是指: 给定 3 个群元素 g, ag 和 $bg \in G$ (a 和 b 为整数), 找出元素 $h \in G$, 使得 $h = (ab)g$.

(c) DDHP (Decision Diffie-Hellman 问题) 是指: 给定 4 个群元素 g, ag, bg 和 cg (a, b 和 c 为整数), 决定是否 $c \equiv ab \pmod{o(g)}$, $o(g)$ 记 g 的阶.

显然有 DHP 意味着 DDHP, 而 DLP 意味着 DHP. 我们以后要考虑的是反过来的蕴涵关系如何, 或者考虑如何解决上述 3 个问题. 在本节前半部分, 主要考虑如何利用 Tate 对解决 DLP. 下面考虑 DDHP:

由前面的讨论, 若域 $k = \mathbb{F}_q$ 含有 l 次单位根, E/k 是一条椭圆曲线, E 有一个阶为 l 的 k 有理点 P, 则此时 Tate 对有定义 (见定理 18.25 或 18.28), 且 $\langle P, P\rangle$ 的值在 $k^*/k^{*l} \cong \mu_l$ 中. 若这个值非平凡, 例如, $\langle P, P\rangle = \zeta_0$, 则 Tate 对提供了一个 DDHP 的简单解法:

设 nP, mP 和 $Q = aP \in \langle P\rangle$, 我们想确定 $Q = mnP$ 是否成立, 为此, 我们计算两次 Tate 对: 首先计算 $\langle nP, mP\rangle = \langle P, P\rangle^{mn}$, 比较这个值与 $\langle P, Q\rangle$ 的值, 若 Q 等于 mnP, 则这两个值应该相等 (因为 $\langle P, Q\rangle = \langle P, aP\rangle = \zeta_0^a$). 因此, 若 $\zeta_0^a = \zeta_0^{nm}$, 则 $a \equiv mn \pmod{l}$. 更进一步, 这个过程仅需要 $\log q$ 的多项式时间 (因为由定理 18.29, Tate 对可在 $O(\log l)$ 步内算出, 而由于 Tate 对的值是 $\mathbb{F}_q^*$ 中的元素, 故比较过程可在 $O(\log q)$ 步内完成).

注意, 若 k 含有一个 l 次单位根, 且 $E(k)[l] = \langle P\rangle$, P 是一个 l 阶点, 则 E/k 的 Tate 对满足 $\langle P, P\rangle \neq 1$. 例如, 由定理 18.30, 这个条件被下述所有椭圆曲线满足: E/k 是迹为 2 的椭圆曲线, 其中 k 含有 l 次单位根, 但不含任何 l^i 次单位根 (对一切 $i \geqslant 2$).

若 E 是 $\mathbb{F}_p$ 上的超奇异椭圆曲线, 可以证明 Tate 对满足 $\langle P, P\rangle = 1$ (对所有 P), 从而 Tate 对不能像上面所述直接应用于 DDHP. 但是, 通过应用 $\mathbb{F}_p$ 上椭圆曲线 E 的自同态环的知识, 有时仍能够应用 Tate 对到该问题.

例 18.5 设 $E/\mathbb{F}_p: y^2 = x^3 + x$, $p \equiv 3 \pmod 4$, 这时候 $E/\mathbb{F}_p$ 是超奇异的. 于是 $|E| = p + 1$, 从而 $E[l]$ ($l \neq 2$) 不能够定义在 $\mathbb{F}_p$ 上 (否则, 有 $l|p-1$ 且 $l|p+1$, 从而 $l|p+1-(p-1)=2$). 从而 $E(\mathbb{F}_p)[l] = \langle P\rangle$ 且 $E(K)[l] = \langle P, Q\rangle$, 此处 $K = \mathbb{F}_{p^2}$, Q 定义在 K 上. 由于 $p \equiv 3 \pmod 4$, 从而 -1 是模 p 的 2 次非剩余, 因此有自同态

$$\phi: \quad (x, y) \longmapsto (-x, iy),$$

此处 i 是 $x^2 + 1 = 0$ 在 K 中的根, ϕ 不定义在 $k = \mathbb{F}_p$ 上. 于是在 E/K 上考虑 Tate

对, 则 $\langle P, \phi(P)\rangle \neq 1$ (否则, 因 $\langle P, P\rangle = 1$, Tate 对在 E/K 上是退化的, 与定理 18.25 矛盾). 由于 ϕ 是同态, 故可通过计算解决 DDHP 如下:

$$\langle aP, \phi(bP)\rangle = \langle aP, b\phi(P)\rangle = \langle P, \phi(P)\rangle^{ab},$$

和

$$\langle cP, \phi(P)\rangle = \langle P, \phi(P)\rangle^{c}.$$

注意, 尽管 Tate 对不是定义在 k 上, 但我们还是可以在 k 的 l 阶子群内解决 DDHP.

注意自同态的应用 (将基域 k 中一个点映射到 k 的一个扩域 K 中一个点) 仅仅在超奇异情形时才可能, 这是因为只有此时的自同态环是非交换的. 下表中列出了一些超奇异椭圆曲线及其上的自同态:

域	曲线	自同态	条件	群阶
$\mathbb{F}_p$	$y^2 = x^3 + ax$	$(x, y) \mapsto (-x, iy)$, $i^2 = -1$	$p \equiv 3 \pmod 4$	$p+1$
$\mathbb{F}_p$	$y^2 = x^3 + a$	$(x, y) \mapsto (\zeta x, y)$, $\zeta^3 = 1$	$p \equiv 2 \pmod 3$	$p+1$
$\mathbb{F}_{p^2}$	$y^2 = x^3 + a$	$(x, y) \mapsto (\omega \frac{x^p}{r^{(2p-1)/3}}, \frac{y^p}{r^{p-1}})$ $r^2 = a$, $r \in \mathbb{F}_{p^2}$, $\omega^3 = r$, $\omega \in \mathbb{F}_{p^6}$	$p \equiv 2 \pmod 3$	$p^2 - p + 1$

一般地, 利用例 18.5 的思想可以证明

定理 18.31 *设 E 是定义在 $\mathbb{F}_q$ 上的超奇异椭圆曲线, 假定 $q = p^f$, f 为奇数, 并假设存在 E 的自同态 $\phi \notin \mathbb{Z} \cdot id_E$ 且 ϕ 限制到 l 阶点可在多项式时间内计算出, 则在 $E(\mathbb{F}_q)[l]$ 中的DDHP可用Tate对解决.*

下面讨论 DLP 和 DHP 之间的关系. 显然的事实是 DLP 蕴含 DHP, 现在讨论反过来的关系.

假设有一个阶为素数 p 的群 G, 以及对于 G 中 DHP 的一个预言器 (oracle). 又假定有一循环椭圆曲线 $E_{a,b}/\mathbb{F}_p$, 且 P 为其生成元, 更设 $E_{a,b}$ 的群阶是 B 光滑的. 在这些假定下, 我们来说明 G 中的 DLP 可在 $\sqrt{B}(\log p)^{O(1)}$ 时间内求得.

假设有 g^x (g 为 G 的生成元), 要求 x. 首先计算群元素 g^{x^3+ax+b}, 这可以在 $O(\log p)$ 个群运算和两次启用 G 中对于 DHP 的预言器 (为了从 g^x 计算 g^{x^3}) 而完成. 若 $x^3 + ax + b$ 是模 p 的 2 次剩余, 则可找到群元素 g^y, 使得 $y^2 \equiv x^3 + ax + b \pmod p$ (否则, 用 g^{x+d} 代替 g^x, d 为随机的). 于是 $Q = (x, y)$ 是 $E_{a,b}$ 上的一个 $\mathbb{F}_p$ 有理点, 而且 $(g^x, g^y) = (g^x, g^{\sqrt{x^3+ax+b}})$. 给定 (g^{u_i}, g^{v_i}), 此处 (u_i, v_i) 是 $E_{a,b}$ 上两个点 ($i = 1, 2$), 则通过 G 中 $O(\log p)$ 个群运算和启用 G 中对 DHP 的预言器 $O(\log p)$ 次, 就能够算出 (g^{u_3}, g^{v_3}), 使得 $(u_3, v_3) = (u_1, v_1) + (u_2, v_2)$. 设 q 是 $|E_{a,b}|$ 的一个素因子, 给定 (g^x, g^y), 计算 (g^u, g^v), 使得在 $E_{a,b}$ 上 $(u, v) = (|E_{a,b}|/q)Q$. 由于 $E_{a,b}$ 的生成元 P 是已知的, 故可以计算点 $(u_i, v_i) = i(|E_{a,b}|/q)P \in E$, $i = 0, 1, \cdots, q-1$

(由于 $|E_{a,b}|$ 的光滑性, 这样的计算是可以的). 从这些 (u_i, v_i) 可以计算出 G 中元素 (g^{u_i}, g^{v_i}).

我们的最终目的是解 G 中 DLP, 而借助于 (g^x, g^y), $(x, y) = Q \in E$, 它转化为 E 上的 DLP.

设 $Q = kP$, 则 $(g^u, g^v) = (g^{u_i}, g^{v_i})$ 当且仅当 $k \equiv i \pmod q$. 但这意味着事实上可以计算出 k 模去 $|E_{a,b}|$ 的每一个素因子的值. 再应用中国剩余定理, 就可以算出 k. 一旦 k 知道, 则可计算 kP, 从而知道 $Q\,(= kP)$. 而 G 中的 DLP 的解由 Q 的第 1 个坐标给出. 由于假定 $E_{a,b}$ 是 B 光滑的, 不难看出这些计算可在 $O(\sqrt{B}(\log p)^3)$ 个运算和启用 $O(\sqrt{B}(\log p)^3)$ 个 DHP 的预言器后完成.

上述思想可以加以推广, 而证明下述定理:

定理 18.32 *设 P 是一固定的多项式, $G = \langle g \rangle$ 为一循环群, $|G| = \prod_{i=1}^{s} p_i^{e_i}$ 已知 (即已知 $|G|$ 及其素因子分解). 令 $B = P(\log|G|)$, 若 $|G|$ 的每一个大于 B 的素因子 p 是单的, 且对每一个这样的 p, 给定一个有限 Abel 群 H_p, 使得 H_p 的秩 (rank) $= O(1)$ 且它在 $\mathbb{F}_p$ 上是强代数定义的, 又假设 H_p 的阶是 B 光滑的 (已知的), 则 G 中关于 g 的DHP是概率多项式时间等价于 G 中关于基 g 的DLP.*

在定理 18.32 的叙述中, 所谓一个有限群 H 是在 $\mathbb{F}_p$ 上 (m, α) 代数定义的, 若 H 中每一个元素可表示为 $\mathbb{F}_p$ 中元素的一个 m' 有序对 $(m' \leqslant m)$, 使得在此表示下, 群运算可由 $\mathbb{F}_p$ 中至多 α 个代数运算完成. 而所谓 H 是 (m, α) 强代数的, 是指 H 是 (m, α) 代数的, 且存在两个算法 λ 和 β, 具有下述性质:

1. $\forall (x, e) \in \mathbb{F}_p^2$, $\lambda(x, e)$ 或者输出 H 的一个元素, 或者报告失败;
2. 若 λ 对输入 (x, e) 运行 (其中 x 固定, e 随机), 直到 λ 不失败, 则直到计算出一个元素 $c \in H$ 的期望的运行时间最多为 $\mathbb{F}_p$ 中 α 个代数运算;
3. 若 $\lambda(x, e)$ 不失败, 则 $\beta(\lambda(x, e), e) = x$;
4. β 的运算时间最多为 α.

例如, 前面的 $E_{a,b}/\mathbb{F}_p$ 就是一个 $(2, O((\log p)^2))$ 强代数定义的. 事实上, $E_{a,b}$ 中每一个点均可表示为 $\mathbb{F}_p$ 中的有序对, 而群运算则在此表示下可由 (常数多个)$\mathbb{F}_p$ 中的加、乘、除和等式检测完成. 下面描述 λ 和 β. 对于 $(x, e) \in \mathbb{F}_p^2$, 计算 $D = (x+e)^3 + a(x+e) + b$, 并检测其是否为 2 次剩余. 若 D 非 2 次剩余, $\lambda(x, e)$ 报告失败, 若 D 是 2 次剩余, 则计算 D 的一个平方根 y, 而 $\lambda(x, e) = (x+e, y)$. 这个过程需要 $O((\log p)^2))$ 个 $\mathbb{F}_p$ 中的代数运算, 而 $\beta((x, y), z) = x - z$, 其中 $(x, y) \in E_{a,b}$, $z \in \mathbb{F}_p$.

定理 18.32 的证明请参见文献 [73].

由于 $E_{a,b}/\mathbb{F}_p$ 是强代数定义的, 为了证明 DHP 和 DLP 的等价性, 由定理 18.32, 还需要在 Hasse 区间 $[p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ 中光滑数分布的一个结果, 但这方面没有什么好的结果. 记 $v(n)$ 是区间 $[n+1-2\sqrt{n}, n+1+2\sqrt{n}]$ 中任意整数 d 的

最大素因子的最小者, 即

$$v(n) = \min\{p|p\text{为 } d \text{ 的最大素因子, 而 } d \text{ 跑遍区间 } [n+1-2\sqrt{n}, n+1+2\sqrt{n}]\},$$

则由前面的讨论, 有下述

定理 18.33 设 P 是一固定的多项式, 对每一个阶为 $|G| = \prod p_i^{e_i}$ 的循环群 G($|G|$ 的重素因子都小于 $P(\log|G|) = B$), 存在一个算法, 它启用 G 中一个DHP预言器并且可在

$$\max\{v(p_i)\} \cdot (\log|G|)^{O(1)}$$

时间内计算出 G 中元素的DLP.

猜想 18.1 $v(n) = (\log n)^{O(1)}$.

若猜想 18.1 成立, 则定理 18.33 意味着存在一个 $\log|G|$ 的多项式算法, 将 G 中 DLP 约化到 G 中 DHP 问题.

注记: 利用代数数论的方法计算离散对数是由 G.Frey 教授提出的. 本章的主要内容的写作参考了 G.Frey 教授的一些讲义和他的一些学生的学位论文.

第五部分

椭圆曲线密码体制的实现

第十九章　椭圆曲线的倍点计算

从前面第一章可知, 椭圆曲线上的有理点有加法运算, 并且在这个加法的意义下构成一个群, 设 P 是椭圆曲线上的一个点, 将 P 自身相加 k 倍的运算

$$[k]P = \underbrace{P \oplus P \oplus \cdots \oplus P}_{k\text{ 个}}$$

称为倍点运算 (scalar multiplication). 在椭圆曲线公钥密码中, 核心运算就是椭圆曲线的倍点运算, 本章介绍常用的计算倍点的算法.

椭圆曲线的倍点运算类似 RSA 公钥密码体制中的模大整数 N 的幂运算, 因此模 N 幂运算的一些方法, 如二进制法、窗口法都可以直接照搬过来, 用于椭圆曲线的倍点运算. 另外, 由于椭圆曲线自身的特殊性, 使得与模 N 幂运算相比, 有如下几方面的优点:

(1) 可以选择适合软件或硬件实现的有限域及椭圆曲线. 在 RSA 公钥密码中, 由于安全性的要求, 参数 $n = pq$ 的素数 p 和 q 不能任意选择. 而椭圆曲线密码体制中, 可以在不影响安全性的前提下选择合适的有限域和具体的椭圆曲线.

(2) 椭圆曲线点的加法和减法的计算量是相当的, 因此在倍点运算中可以使用加减法, 而模 N 幂运算中, 求逆运算要比乘法运算慢得多.

(3) 利用椭圆曲线的复乘. 在一类特殊的椭圆曲线中 (例如 Koblitz 曲线), 有所谓的 Frobenuis 展开式, 利用 Frobenius 展开式, 可以有效地计算倍点运算.

§19.1　基域和曲线的选择

在实际应用中, 基域有两种选择: 1. $\mathbb{F}_p = \mathbb{Z}_p = \{0, 1, 2, \cdots, p-1\}$, 其中 p 为大素数, 即特征 p 的有限域; 2. $\mathbb{F}_{2^n}$, 即特征 2 的有限域. 前者适合于软件实现, 而后者适合于硬件实现.

一、特征 p 的有限域

在 $\mathbb{F}_p$ 中要用到加、减、乘和求逆运算, 其中加法和减法运算的速度相对很快, 在算法分析中总是忽略不计.

乘法运算是先进行乘法, 再利用除法, 求得模 p 的余数, 从而得到最后的结果. 除法的速度一般比较慢, 因此对于一般的素数 p 来说, 有限域中乘法的速度比较慢. 但是这可以通过选择特殊形式的素数 p 来提高有限域中乘法的速度, 而且到目前为

止, 对于特征 p 的椭圆曲线公钥密码, 还没有发现因有限域的选择而造成的安全性隐患, 即, 还没有发现因有限域 p 的选择而导致椭圆曲线离散对数容易计算的情形。因此, 在实际应用中, 往往选择适合于软件实现的素数 p. 一般来说有两种选择:

(1) p 形如 $2^k \pm \alpha$.　α 是很小的整数, 这样的素数称为拟 Mersenne 素数. 在这种情形下, $2^k \equiv \mp\alpha \pmod p$, 因此要计算 $t \bmod p$, 先将 t 写成

$$t = t_l + t_h 2^k,$$

从而 $t \equiv t_1 \mp \alpha * t_h \pmod p$. 如果结果仍然不小于 p, 则重复使用上述方法, 就可以快速计算 $t \bmod p$. 因此有如下的算法:

(算法 19.1)　约化算法

输入: 整数 t.

输出: $t \bmod p$ 为不超过 p 的最小非负整数.

Step 1. s=t;

Step 2. Whie $s \geqslant p$

　　Step 2.1 $m = s \bmod 2^k$;　　/* 取 s 除以 2^k 的余数 */

　　Step 2.2 $l = s/2^k$;　　/* 求 s 除以 2^k 的商 */

　　Step 2.3 $s = m \mp \alpha * l$

Step 3. 输出 s.

在实际应用中, k 点取为计算机字长的倍数. 例如目前普遍认为 192 比特的椭圆曲线是安全的, 因此可取 $k = 192$. 而整数在计算机中的表示是采用 2^w 进制, 即

$$t = t_0 + t_1 2^w + t_2 2^{2w} + \cdots + 2^{k-1} 2^{(k-1)w} + \cdots,$$

其中 w 为计算机字长, 一般取为 $w = 32$ 或 64. 在这种表示下, 算法中的第 2.1 步和 2.2 步的计算是容易的, 只需要截取相应的部分即可.

例 19.1　取 $p = 2^5 - 1 = 31$, 计算 $t = 1005$ 模 p 的最小非负余数.

解　因为 $t = 1005 = 13 + 31 * 32$, 因此

$$t \equiv 13 + 31 = 12 + 1 * 32 \equiv 13 \pmod p.$$

事实上, $1005 = 32 * p + 13$.

这样的拟 Mersenne 素数很多, 例如 160 比特的拟 Mersenne 素数有

$p_1 = 2^{160} - 47 = 1461501637330902918203684832716283019655932542929,$

$p_2 = 2^{160} + 7 = 1461501637330902918203684832716283019655932542983.$

192 比特的拟 Mersenne 素数有

$$p_3 = 2^{192} - 237$$
$$= 6277101735386680763835789423207666416102355444464034512659,$$
$$p_4 = 2^{192} + 133$$
$$= 6277101735386680763835789423207666416102355444464034513029.$$

256 比特的拟 Mersenne 素数有

$$p_5 = 2^{256} - 189 = 115792089237316195423570985008687907853269 9\backslash$$
$$84665640564039457584007913129639747,$$
$$p_6 = 2^{256} + 297 = 115792089237316195423570985008687907853269 9\backslash$$
$$84665640564039457584007913129640233.$$

(2) p 形如 $2^k \pm 2^s \pm 1$. 其中 k, s 是计算机字长的倍数 (如 8, 16, 32, 64). 这样的素数不是太多, 160 比特的这种素数不存在; 192 比特的这种素数有如下几个 (其中 p_2 是 NIST 在数字签名标准中推荐使用的):

$$p_1 = 2^{192} - 2^{16} - 1$$
$$= 6277101735386680763835789423207666416102355444464034447359,$$
$$p_2 = 2^{192} - 2^{64} - 1$$
$$= 6277101735386680763835789423207666416083908700390324961279,$$
$$p_3 = 2^{192} + 2^{120} - 1$$
$$= 6277101735386680763837118651203451331975259251524314857471,$$
$$p_4 = 2^{192} + 2^{184} - 1$$
$$= 6301621664040534985569522975642071363040255270418972147711.$$

而 256 比特的这种素数只有如下两个:

$$p_1 = 2^{256} + 2^{96} - 1 \quad = 115792089237316195423570985008687907853269 9\backslash$$
$$84665719792201971848345506673590271,$$
$$p_2 = 2^{256} - 2^{168} + 1 = 115792089237316195423570984634543488696558 8\backslash$$
$$37605497246864089130975994398638081.$$

对于这种素数, 也有类似拟 Mersenne 素数的快速约化算法, 只不过在这种情形下, 只是进行一些相应字的加加减减, 效率还高于第 1 种情形的拟 Mersenne 素数. 由于分析的方法完全一样, 下面仅以 $p = 2^{192} - 2^{96} - 1$ 为例, 说明模 p 的约化算法:

令 $A = A_0 + A_1 \cdot 2^{192}$ 是小于 p^2 的整数, 因为 $2^{192} \equiv 2^{64} + 1 \pmod p$, 故

$$A = A_0 + A_1 \cdot 2^{192} \equiv A_0 + A_1 \cdot 2^{64} + A_1 \pmod p.$$

为了进一步约化, 令

$$A = a_0 + a_1 \cdot 2^{64} + a_2 \cdot 2^{128} + a_3 \cdot 2^{192} + a_4 \cdot 2^{256} + a_5 \cdot 2^{320},$$

经过简单的计算, 有

$$\begin{aligned} A \equiv a_0 + a_1 \cdot 2^{64} + a_2 \cdot 2^{128} + a_3 + a_4 \cdot 2^{64} + a_5 \cdot 2^{128} \\ + a_3 \cdot 2^{64} + a_4 \cdot 2^{128} + a_5 + a_5 \cdot 2^{64} \pmod p. \end{aligned}$$

如果令

$$\begin{aligned} A_0 &= a_0 + a_1 \cdot 2^{64} + a_2 \cdot 2^{128}, \qquad & S_1 &= a_5 + a_5 \cdot 2^{64} + a_5 \cdot 2^{128}, \\ S_2 &= a_3 + a_3 \cdot 2^{64}, & S_3 &= \qquad a_4 \cdot 2^{64} + a_4 \cdot 2^{128}, \end{aligned}$$

则 $A = A_0 + S_1 + S_2 + S_3 \pmod p$(注意所有的运算只是在相应的位置加上相应的计算机字).

由于这样的素数比较少, 有时也考虑具有 5 项的这种形式的素数, 而 NIST 所推荐的例子都是这种形式的素数.

有限域中的求逆运算往往是用扩展 Euclid 除法, 速度很慢, 但是在实际应用中, 往往采用椭圆曲线的 Jacobi 坐标代替一般的仿射坐标, 牺牲几个有限域中的乘法来避免求逆运算.

二、特征 2 的有限域

有限域 $\mathbb{F}_{2^n}$ 可以看成 $\mathbb{F}_2$ 上的向量空间, 元素的加法实际上是各分量之间的按位异或, 这样的有限域比较适合于硬件实现. 有限域 $\mathbb{F}_{2^n}$ 有两种常用的表示方法: (1) 多项式基; (2) 正规基. .

(1) 有限域 $\mathbb{F}_{2^n}$ 的多项式基. 对于任意给定的 $n \geqslant 1$, 总存在 $\mathbb{F}_2[x]$ 上的 n 次不可约多项式 $f(x)$, 则 $\mathbb{F}_{2^n} \cong \mathbb{F}_2[x]/(f(x))$, $\mathbb{F}_{2^n}$ 也可以看作将 $f(x)$ 的一个根 α 添加到 $\mathbb{F}_2$ 上所得到的最小扩域. 有限域 $\mathbb{F}_{2^n}$ 实际上是 $\mathbb{F}_2$ 上的 n 维向量空间, 设 α 是 $f(x)$ 在 $\mathbb{F}_{2^n}$ 中的一个根, 则 $\{1, \alpha, \alpha^2, \cdots, \alpha^{n-1}\}$ 在 $\mathbb{F}_2$ 上线性无关, 构成向量空间的一组基, 称为多项式基. 在多项式基表示下, $\mathbb{F}_{2^n}$ 中的元素可看成次数小于 n 的多项式.

$\mathbb{F}_{2^n}$ 中的乘法运算是先按照多项式的规则计算乘积, 得到一个 $2n-2$ 次的多项式, 再利用带余除法, 计算除以 $f(x)$ 后的余数, 即为乘法结果. 为了加速乘法运算, 可以如下地选择不可约多项式 $f(x)$:

(a) $f(x)$是稀疏多项式. 即 $f(x)$ 中的非零项比较少, 特别地, 可选择 3 项式或 5 项式, 这样可以提高求余运算的效率, P1363 [74] 中列表说明, 对于任意的 $n \leqslant 1000$, 如果不存在次数为 n 的 3 项式的话, 则一定存在次数为 n 的 5 项式. 下面给出 3 项式的求余算法 (事实上是带余除法的另外一种写法), 其中 $f(x) = x^n+x^t+1,\ 0 < t < n$.

输入: $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{2n-2}x^{2n-2} \in \mathbb{F}_2[x]$.

输出: $r(x) \equiv a(x) \pmod{f(x)}$, $\deg r(x) < n$.

1. For $i = 2n-2$ to n do;

 1.1 $a_{i-n} = a_{i-n} + a_i$, $a_{i-n+t} = a_{i-n+t} + a_i$;

2. 输出 $r(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$.

例 19.2 $f(x) = x^5+x^2+1$ 是不可约多项式, 令 $a(x) = 1+x^2+x^4+x^5+x^7+x^8$, 求 $r(x) \equiv a(x) \pmod{f(x)}$, 且 $\deg r(x) < 5$.

解 将上面算法中经过每一步后的各系数变化情况列表如下:

	a_8	a_7	a_6	a_5	a_4	a_3	a_2	a_1	a_0
初始	1	1	0	1	1	0	1	0	1
$i=8$	0	1	0	0*	1	1*	1	0	1
$i=7$	0	0	0	0	0*	1	0*	0	1
$i=6$	0	0	0	0	0	1	0	0	1
$i=5$	0	0	0	0	0	1	0	0	1

(其中星号表示发生改变的位置, 而第 i 位在第 i 步后是舍弃的, 因此表中都置为 0), 因此 $r(x) = x^3 + 1$.

(b) 选择 $f(x) = x^n + g(x)$. 其中 $g(x)$ 的次数比较小. 对于这种多项式, 可以采用类似拟 Mersenne 素数的方法处理, 这里从略.

有限域 $\mathbb{F}_{2^n}$ 中的平方运算有比较快的方法. 设 $a(x) = a_0 + a_1x + a_2x^2 + \cdots + a_{n-1}x^{n-1}$, 则

$$a(x)^2 = a(x^2) = a_0 + a_1x^2 + a_2x^4 + \cdots + a_{n-1}x^{2n-2}.$$

如果选择上面介绍的域定义多项式, 则可以用上面的算法进行约化. 如果 $f(x)$ 是一个一般的不可约多项式, 则可以对 $n \leqslant 2i < 2n-2$, 先预计算 $x^{2i} \equiv r_i \pmod{f(x)}$, 其中 $\deg r_i(x) < n$, 再进行平均 $n/2$ 个 $\mathbb{F}_{2^n}$ 中的加法运算即可完成整个平方运算.

(2) 有限域 $\mathbb{F}_{2^n}$ 的正规基. 如果存在 $\alpha \in \mathbb{F}_{2^n}$, 使得 $\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{n-1}}\}$ 线性无关, 则称之为有限域 $\mathbb{F}_{2^n}$ 的一组正规基. 易知, 对于任意的正整数 $n \geqslant 1$, 总存在 $\mathbb{F}_{2^n}$ 的正规基 (可参阅 Lidl 和 Niederreiter 的书[41], 第二章, 定理 2.35). 正规基对于硬件实现有优势: (i) $\mathbb{F}_{2^n}$ 中的平方运算实际上是移位运算; (ii) 对于域中的一般乘法, 可以转换为一系列的位操作, 这对于软件实现比较困难, 但对于硬件实现就非常容易. 下面介绍 $\mathbb{F}_{2^n}$ 在正规基下的乘法运算:

设 $\beta = a_0\alpha + a_1\alpha^2 + a_2\alpha^{2^2} + \cdots + a_{n-1}\alpha^{2^{n-1}}$, $\gamma = b_0\alpha + b_1\alpha^2 + b_2\alpha^{2^2} + \cdots + b_{n-1}\alpha^{2^{n-1}}$, 则

$$\begin{aligned}\beta\cdot\gamma &= \sum_{i=0}^{n-1} a_ib_i\alpha^{2^{i+1}} + \sum_{0\leqslant i<j\leqslant n-1}(a_ib_j + a_jb_i)\alpha^{2^i+2^j}\\ &= \sum_{i=0}^{n-1} a_ib_i\alpha^{2^{i+1}} + \sum_{0\leqslant i<j\leqslant n-1}(a_ib_j + a_jb_i)\left(\alpha^{2^{j-i}+1}\right)^{2^i}.\end{aligned}$$

为了计算元素的乘法, 需要对每个 $0\leqslant i\leqslant n-1$, 将 α^{2^i+1} 表示成 $\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{n-1}}$ 的线性组合

$$\alpha^{2^i+1} = \sum_{j=0}^{n-1} T_{ij}\alpha^{2^i}, \quad T_{ij} = 0, 1,$$

因此, 矩阵 $(T_{ij})_{n\times n}$ 中 1 的个数 C_α 的多少决定了计算 $\mathbb{F}_{2^n}$ 中一般乘法的复杂性. 一方面, $C_\alpha \leqslant n^2$ 是显然的. 另一方面, 可以证明 C_α 满足下界 $C_\alpha \geqslant 2n-1$ (可参阅文献 [75]). 称满足下界 $C_\alpha = 2n-1$ 的正规基为最优正规基. 下面的定理说明了最优正规基的存在性:

定理 19.1　(1) 如果 $n+1$ 是素数, 且 2 是模 $n+1$ 的原根, 则 $\mathbb{F}_{2^n}$ 中 n 个不是 1 的 $n+1$ 次单位根就构成 $\mathbb{F}_{2^n}$ 的最优正规基, 这样的最优正规基称为第1类型的最优正规基.

(2) 如果 $2n+1$ 是素数, 并且下面两个条件之一成立:

(a) 2 是模 $2n+1$ 的原根;

(b) $2n+1\equiv 3 \pmod 4$ 且 2 模 $2n+1$ 的阶为 n.

令 γ 是模 $2n+1$ 的原根, 则 $\alpha = \gamma + \gamma^{-1}$ 就产生 $\mathbb{F}_{2^n}$ 的一组最优正规基, 这样的最优正规基称为第 2 类型的最优正规基.

证明可参阅文献 [75].

例 19.3　令 $n=4$, 考虑有限域 $\mathbb{F}_{2^4}$, 易知 $f(x) = x^4 + x + 1$ 是 $\mathbb{F}_2[x]$ 中的不可约多项式, 因此 $f(x)$ 可作为 $\mathbb{F}_{2^4}$ 的域多项式. 令 β 是 $f(x)=0$ 的一个根, 则

$$\mathbb{F}_{2^4} = \{a_0 + a_1\beta + a_2\beta^2 + a_3\beta^3 \mid a_0, a_1, a_2, a_3 \in \mathbb{F}_2\}.$$

$\mathbb{F}_{2^4}$ 中的乘法表如下:

$\beta^0 = 1$	$\beta^5 = \beta + \beta^2$	$\beta^{10} = 1 + \beta + \beta^2$
$\beta^1 = \beta$	$\beta^6 = \beta^2 + \beta^3$	$\beta^{11} = \beta + \beta^2 + \beta^3$
$\beta^2 = \beta^2$	$\beta^7 = 1 + \beta + \beta^3$	$\beta^{12} = 1 + \beta + \beta^2 + \beta^3$
$\beta^3 = \beta^3$	$\beta^8 = 1 + \beta^2$	$\beta^{13} = 1 + \beta^2 + \beta^3$
$\beta^4 = 1 + \beta$	$\beta^9 = \beta + \beta^3$	$\beta^{14} = 1 + \beta^3$

因 $n+1=5$ 是素数, 且 2 是模 5 的原根, 令 $\alpha=\beta^3$, 由定理 19.1 的 (1) 知,

$$\{\alpha,\alpha^2,\alpha^4,\alpha^8\}$$

是域 $\mathbb{F}_{2^4}$ 的一组最优正规基. 事实上, 由乘法表, 不难得到如下的矩阵:

$$\begin{pmatrix}\alpha^{1+2^0}\\ \alpha^{1+2^1}\\ \alpha^{1+2^2}\\ \alpha^{1+2^3}\end{pmatrix}=\begin{pmatrix}0&1&0&0\\0&0&0&1\\1&1&1&1\\0&0&1&0\end{pmatrix}\begin{pmatrix}\alpha\\ \alpha^2\\ \alpha^4\\ \alpha^8\end{pmatrix},$$

而 $C_\alpha=7=2\times4-1$, 因而 $\{\alpha,\alpha^2,\alpha^4,\alpha^8\}$ 是 $\mathbb{F}_{2^4}$ 的最优正规基.

设 $\gamma_1=a_0\alpha+a_1\alpha^2+a_2\alpha^4+a_3\alpha^8$, $\gamma_2=b_0\alpha+b_1\alpha^2+b_2\alpha^4+b_3\alpha^8\in\mathbb{F}_{2^4}$, 则

$$\begin{aligned}\gamma_1\cdot\gamma_2&=a_0b_0\alpha^2+a_1b_1\alpha^4+a_2b_2\alpha^8+a_3b_3\alpha\\&\quad+(a_0b_1+a_1b_0)\alpha^3+(a_0b_2+a_2b_0)\alpha^5+(a_3b_0+a_0b_3)\alpha^9\\&\quad+(a_1b_2+a_2b_1)\alpha^6+(a_1b_3+a_3b_1)\beta^{10}+(a_2b_3+a_3b_2)\beta^{12}\\&=[a_0b_2+a_1(b_2+b_3)+a_2(b_0+b_1)+a_3(b_1+b_3)]\alpha\\&\quad+[a_1b_3+a_2(b_3+b_0)+a_3(b_1+b_2)+a_0(b_2+b_0)]\alpha^2\\&\quad+[a_2b_0+a_3(b_0+b_1)+a_0(b_2+b_3)+a_1(b_3+b_1)]\alpha^4\\&\quad+[a_3b_1+a_0(b_1+b_2)+a_1(b_3+b_0)+a_2(b_0+b_2)]\beta^8.\end{aligned}$$

对于一般的正规基, 有限域中的乘法运算还是很复杂的, 因此在实际应用的时候, 往往要选择适当的正规基 (即上文的矩阵中非零项越少越好). 为此, 用一个整数 T 表示正规基的类型, 这样的正规基称为高斯正规基. 如果 n 不能被 8 整除, 则可以用下面的算法决断有限域 $\mathbb{F}_{2^n}$ 中是否存在类型 T 的高斯正规基 (可参阅 P1363[74] 的附录 A):

(算法 19.2)　判断类型 T 的高斯正规基是否存在

输入: 有限域 $\mathbb{F}_{2^n}$ 的扩张次数 n 和正整数 T.

输出: 是否存在类型 T 的高斯正规基.

Step 1. 令 $p=nT+1$;

Step 2. 如果 p 不是素数, 则输出 "不存在类型 T 的高斯正规基";

Step 3. 计算有限域 $\mathbb{Z}_p$ 中 2 的阶 $k=\mathrm{ord}(2)$; 即最小的正整数 k, 使得 $2^k\equiv1\pmod p$;

Step 4. 计算 $h = (Tn)/k$;

Step 5. 计算 $d = \gcd(h, n)$;

Step 6. 如果 $d = 1$, 则输出“存在类型 T 的高斯正规基”; 否则, 输出“不存在类型 T 的高斯正规基”.

上面的定理 19.1 就给出了类型为 $T = 1$ 和 2 的高斯正规基的存在条件. 进一步, 如果有限域 $\mathbb{F}_{2^n}$ 中存在类型 T 的高斯正规基 B, 在这组正规基下, 设 $a = (a_0, a_1, \cdots, a_{n-1})$, $b = (b_0, b_1, \cdots, b_{n-1}) \in \mathbb{F}_{2^n}$, 令 $c = (c_0, c_1, \cdots, c_{n-1}) = ab$, 则下面的算法给出有限域 $\mathbb{F}_{2^n}$ 中乘法的第 1 个坐标公式 c_0:

(算法 19.3) 计算正规基表示下乘法的第 1 个坐标

输入: n, T 使得在 $\mathbb{F}_{2^n}$ 中存在类型 T 的高斯正规基.

输出: ab 的第一个坐标 c_0.

Step 1. 令 $p = nT + 1$;

Step 2. 计算整数 u, 使得在有限域 $\mathbb{Z}_p$ 中, u 的阶为 T;

Step 3. 按照下面的方法计算 $F(1), F(2) \cdots, F(p-1)$:

Step 3.1 令 $w = 1$;

Step 3.2 For j from 0 to $T-1$ do

令 $s = w$;

For i from 0 to $n-1$ do

$F(s) = i, \quad s = 2s \pmod p$;

令 $w = uw \pmod p$;

Step 4. 如果 T 是偶数, 令 $J = 0$, 否则, 令

$$J = \sum_{k=1}^{n/2} (a_{k-1} b_{n/2+k-1} + a_{n/2+k-1} b_{k-1});$$

Step 5. 令

$$c_0 = J + \sum_{k=1}^{p-2} a_{F(k+1)} b_{F(p-k)};$$

Step 6. 输出 c_0.

例 19.4 考虑有限域 $\mathbb{F}_{2^4}$, 利用算法 19.2 可知 $\mathbb{F}_{2^4}$ 中存在类型 $T = 3$ 的高斯正规基 (因为 $p = 3 * 4 + 1 = 13$ 是素数, 且 2 模 13 的阶为 12, 则 $h = 1$, 因此

$d = \gcd(h, n) = 1$). 再利用算法 19.3, 可得

$$\begin{array}{llll} F(1) = 0, & F(4) = 2, & F(7) = 3, & F(10) = 2, \\ F(2) = 1, & F(5) = 1, & F(8) = 3, & F(11) = 3, \\ F(3) = 0, & F(6) = 1, & F(9) = 0, & F(12) = 2. \end{array}$$

因此, 如果 $a = (a_0, a_1, a_2, a_3)$, $b = (b_0, b_1, b_2, b_3)$, $c = ab = (c_0, c_1, c_2, c_3)$, 可知

$$c_0 = a_0(b_1 + b_2 + b_3) + a_1(b_0 + b_2) + a_2(b_0 + b_1) + a_3(b_0 + b_3).$$

又由于

$$c^2 = (c_3, c_0, c_1, c_2) = a^2 \cdot b^2 = (a_3, a_0, a_1, a_2) \cdot (b_3, b_0, b_1, b_2),$$

再利用算法 19.3 可得

$$c_3 = a_3(b_0 + b_1 + b_2) + a_0(b_3 + b_1) + a_1(b_3 + b_0) + a_2(b_3 + b_2).$$

重复利用上面的方法可得

$$\begin{aligned} c_1 &= a_1(b_2 + b_3 + b_0) + a_2(b_1 + b_3) + a_3(b_1 + b_2) + a_0(b_1 + b_0), \\ c_2 &= a_2(b_3 + b_0 + b_1) + a_3(b_2 + b_0) + a_0(b_2 + b_3) + a_1(b_2 + b_1). \end{aligned}$$

注记 19.1 在例 19.3 中, 采用的是最优正规基, 即类型 $T = 1$ 的高斯正规基, 而例 19.4 中, 采用的是类型 $T = 3$ 的高斯正规基, 因此前者的计算公式要比后者的计算公式简单些.

例 19.5 利用算法 19.2, 很容易计算一些有限域 $\mathbb{F}_{2^n}$, 以及其上存在何种类型的高斯正规基:

n	163	167	173	179	181	191	193	197	199
T	4	14	2	2	6	2	4	18	4

n	211	223	227	229	233	239	241	151	257
T	10	12	24	12	2	2	6	2	6

$\mathbb{F}_{2^n}$ 中的求逆运算有两种方法, 第 1, 扩展 Euclid 除法及其变形; 第 2, 利用 Fermat 小定理, 即对任意 $\beta \in \mathbb{F}_{2^n}^*$, 有

$$\beta^{-1} = \beta^{2^n - 2} = \left(\beta^{2^{n-1} - 1}\right)^2.$$

Itoh 和 Tsufii 在文献 [76] 中提出了一种快速计算的方法, 利用这种方法, 可以减少乘法的运算, 该算法假定 $\mathbb{F}_{2^n}$ 中的平方运算可以忽略不计 (在 $\mathbb{F}_{2^n}$ 的正规基表

示中, 是可以做到这一点的), 并且递归地使用下面的恒等式:

$$\beta^{2^{n-1}-1} = \begin{cases} \beta^{(2^{\frac{n-1}{2}}-1)(2^{\frac{n-1}{2}}+1)} = \left(\beta^{2^{\frac{n-1}{2}}-1}\right)^{2^{\frac{n-1}{2}}} \cdot \beta^{\beta^{2^{\frac{n-1}{2}}}-1}, & n \text{ 是奇数}, \\ \beta\beta^{2^{n-1}-2} = \beta\left(\beta^{2^{n-2}-1}\right)^2, & n \text{ 是偶数}. \end{cases}$$

下面分析一下该算法的计算量, 令 $\mu(n-1)$ 表示计算 $\beta^{\frac{n-1}{2}-1}$ 所需要的乘法的个数. 由上式可得

$$\mu(n-1) = \begin{cases} 1 + \mu\left(\dfrac{n-1}{2}\right), & n \text{ 是奇数}, \\ 1 + \mu(n-2) = 2 + \mu\left(\dfrac{n-2}{2}\right), & n \text{ 是偶数}. \end{cases}$$

当 $n=2$ 时, $\beta^{2^{2-1}-1} = \beta$, 不需要乘法, 因此 $\mu(1)=1$, 当 $n=3$ 时, $\beta^{2^{3-1}-1} = \beta^3 = \beta \cdot \beta^2$ 需要一个乘法, 因此 $\mu(2)=1$, 利用上面的递推公式, 不难知道

$$\mu(n-1) = \lfloor \log_2(n-1) \rfloor + W(n-1) - 1,$$

其中 $W(n-1)$ 表示 $n-1$ 的二进制表达式的重量.

例 19.6　$n=193$, 则 $n-1=192=1\,1\,0\,0\,0\,0\,0\,0$. 利用上面的公式有

$$\begin{aligned} \mu(192) &= 1 + \mu(96) = 2 + \mu(48) = 3 + \mu(24) = 4 + \mu(12) \\ &= 5 + \mu(6) = 6 + \mu(3) = 8 + \mu(1) = 8, \end{aligned}$$

因此在计算 $\beta^{2^{192}-1}$ 时, 按照下面的顺序计算

$$\beta^{2^3-1}, \beta^{2^6-1}, \beta^{2^{12}-1}, \beta^{2^{24}}, \beta^{2^{48}}, \beta^{2^{96}}, \beta^{2^{192}-1}.$$

将上面的方法可写成算法如下:

(算法 19.4)　求逆算法

输入: $\beta \in \mathbb{F}_{2^n}$ 及有限域的扩张次数 n.

输出: $\beta^{2^{n-1}-1}$.

Step 1. 写出 $n-1$ 的二进制表示 $b_r b_{r-1} \cdots b_1 b_0$, $b_r = 1$;

Step 2. $\eta = \beta$, $k = 1$;

Step 3. For $i = r-1$ to 0 do

　　Step 3.1 $\mu = \eta$;

　　Step 3.2 For $j = 1$ to k do　$\mu = \mu^2$;

Step 3.3 $\eta = \mu\eta$, $k = 2k$;

Step 3.4 If $b_i = 1$, do

Step 3.4.1 $\eta = \eta^2\beta$, $k = k + 1$;

Step 4. 输出 η^2.

关于特征 2 的有限域的选择, 需要考虑如下几方面的因素: 首先考虑抵抗椭圆曲线离散对数 (ECDLP): 为了避免 Weil 下降攻击, 有限域 $\mathbb{F}_{2^n}$ 中的 n 应该选择素数; 而为了避免 GHS 攻击, 素数 n 不应为 Fermat 素数或 Mersenne 素数. 其次要考虑实现方面的优点: 如果是选择多项式基, 则最好选择具有 3 项式或 5 项式的 n 次不可约多项式; 如果选择正规基, 则最好选择类型 T 比较小的高斯正规基.

三、椭圆曲线的选择

在实际应用中, 常用的椭圆曲线有两类:

(1) 素数域 $\mathbb{F}_p$, $p > 3$, 此时的椭圆曲线方程为

$$y^2 = x^3 + ax + b, \quad 4a^3 + 27b^2 \not\equiv 0 \pmod p. \tag{19.1}$$

(2) 二元域 $\mathbb{F}_{2^m}$, 此时的椭圆曲线方程为

$$y^2 + xy = x^3 + ax^2 + b, \quad b \neq 0. \tag{19.2}$$

对于特征 p 的情形, 在下一节可以看到, 如果采用 Jacobi 坐标, 当 $a \equiv -3 \pmod p$ 时, 计算椭圆曲线上点的两倍加时可以减少几个有限域中的乘法. 因此, 在选择椭圆曲线 (19.1) 时, 一方面令 $a \equiv -3 \pmod p$, 另一方面, 椭圆曲线的阶 $\#E(\mathbb{F}_p)$ 是个素数, 满足这些条件的椭圆曲线可由本书第五章 SEA 算法来产生.

对于特征 2 的情形, 有两种选择: (1) 基于 §19.4 中介绍的利用 Frobenius 展开式可以有效地计算倍点运算, 因此 Koblitz 建议使用反常椭圆曲线 (anomalous); (2) 在下一节椭圆曲线上点的运算里, 可以看到, 如果椭圆曲线的方程 (19.2) 中的 $a = 0$, 则点的加法计算中, 可以减少一个乘法和一个平方运算, 因此约定 $a = 0$. 利用本书第九章和第十章介绍的 Satoh 算法, 寻找满足上面条件的椭圆曲线, 且使该椭圆曲线上的阶有大的素因子.

§19.2 椭圆曲线上点的表示和运算

在第一章, 已经定义了椭圆曲线上点的加法, 在实际计算中, 椭圆曲线选择的坐标不同, 会影响到计算椭圆曲线上点的加法的运算效率. 本节将比较用不同坐标表示椭圆曲线上点时计算点的加法的计算效率.

有限域 $\mathbb{F}_q$ 中的加法和减法运算的耗时相对于乘法和求逆运算的耗时, 是可以忽略不计的; 另一方面, 对于特征 p 的有限域, 精心设计的平方运算要比一般的乘法运算快将近 20%, 而在特征 2 的有限域中, 如果采用正规基表示, 则平方运算的效率更高. 因此我们在分析计算效率时, 只考虑有限域中的乘法运算、平方运算和求逆运算, 分别用 M, S 和 I 表示, 并分析用不同的坐标如何计算点的加法时所需要的计算量.

一、点的表示

椭圆曲线上的点有几种不同的坐标表示, 不同的坐标表示在计算点的加法和两倍加时运算效率不一样. 通常, 椭圆曲线上点的表示主要有 3 种方式: 仿射坐标、齐次坐标和 Jacobi 坐标, 其中

(1) 仿射坐标: 用 (x,y) 表示椭圆曲线上的点, 而无穷远点用 $\mathcal{O}$ 表示.

(2) 齐次坐标: 用 (X,Y,Z) 表示椭圆曲线上的点, 它与仿射坐标的关系如下:

$$x = X/Z, \quad y = Y/Z,$$

而 $(0,1,0)$ 表示无穷远点.

(3) Jacobi 坐标: 用 (X,Y,Z) 表示椭圆曲线上的坐标, 它与仿射坐标的关系如下:

$$x = X/Z^2, \quad y = Y/Z^3,$$

而 $(0,1,0)$ 表示无穷远点.

约定: 由于射影坐标在实际中应用不多, 因此下面只考虑在仿射坐标和 Jacobi 坐标下点的运算.

从仿射坐标 (x,y) 转换到 Jacobi 坐标 (X,Y,Z), 只需要令 $X=x, Y=y, Z=1$ 即可. 而从 Jacobi 坐标转换到仿射坐标, 需要 $3M+1S+1I$.

二、点的运算

下面分析椭圆曲线点的加法的计算效率, 分两种情形: (1) 特征 p $(p>3)$ 的椭圆曲线; (2) 特征 2 的椭圆曲线.

(1) 特征 $p>3$ 的情形. 椭圆曲线的方程如 (19.1) 所示.

仿射坐标: 设 $P=(x_1,y_1)$, $Q=(x_2,y_2)$, $R=(x_3,y_3)=P+Q$. 如果 $P\neq Q$, 则有如下的加法计算公式:

$$\begin{aligned}
&\lambda = \frac{y_2-y_1}{x_2-x_1}, && 1M+1I,\\
&x_3 = \lambda^2 - x_1 - x_2, && 1S,\\
&y_3 = (x_1-x_3)\lambda - y_1, && 1M.
\end{aligned}$$

因此, 在仿射坐标下, 椭圆曲线点的加法的计算量为 $2M+1S+1I$.

如果 $P=Q$, 则有下面的两倍加的计算公式:

$$\begin{aligned}
\lambda &= \frac{3x_1^2+a}{2y_1}, && 1M+1S+1I,\\
x_3 &= \lambda^2-2x_1, && 1S,\\
y_3 &= (x_1-x_3)\lambda-y_1, && 1M.
\end{aligned}$$

因此, 在仿射坐标下, 椭圆曲线点的两倍加的计算量为 $2M+2S+1I$.

Jacobi 坐标：令 $x=X/Z^2$, $y=Y/Z^3$, 则椭圆曲线的方程为

$$Y^2=X^3+aXZ^4+bZ^6.$$

令 $P=(X_1,Y_1,Z_1)$, $Q=(X_2,Y_2,Z_2)$, $R=(X_3,Y_3,Z_3)=P+Q$, 如果 $P\neq Q$, 采用 P1363 中的算法如下：

$$\begin{aligned}
\lambda_1 &= X_1Z_2^2, && 1M+1S,\\
\lambda_2 &= X_2Z_1^2, && 1M+1S,\\
\lambda_3 &= \lambda_1-\lambda_2, &&\\
\lambda_4 &= Y_1Z_2^3, && 2M,\\
\lambda_5 &= Y_2Z_1^3, && 2M,\\
\lambda_6 &= \lambda_4-\lambda_5, &&\\
\lambda_7 &= \lambda_1+\lambda_2, &&\\
\lambda_8 &= \lambda_4+\lambda_5, &&\\
Z_3 &= Z_1Z_2\lambda_3, && 2M,\\
X_3 &= \lambda_6^2-\lambda_7\lambda_3^2, && 1M+2S,\\
\lambda_9 &= \lambda_7\lambda_3^2-2X_3, &&\\
Y_3 &= (\lambda_9\lambda_6-\lambda_8\lambda_3^3)/2, && 3M.
\end{aligned}$$

因此, 在 Jacobi 坐标下, 加法的计算量是 $12M+4S$, 如果 $Z_2=1$, 则对于 Jacobi 点的加法运算的计算量是 $8M+3S$.

如果 $P=Q$, 则有下面的两倍加的计算公式：

$$\begin{aligned}
\lambda_1 &= 3X_1^2+aZ_1^4, && 1M+3S,\\
Z_3 &= 2Y_1Z_1, && 1M,\\
\lambda_2 &= 4X_1Y_1^2, && 1M+1S,\\
X_3 &= \lambda_1^2-2\lambda_2, && 1S,\\
\lambda_3 &= 8Y_1^4, && 1S,\\
Y_3 &= \lambda_1(\lambda_2-X_3)-\lambda_3, && 1M.
\end{aligned}$$

因此, 在 Jacobi 坐标下, 两倍加的计算量为 $4M+6S$. 如果 $a \equiv -3 \pmod p$, 则 $\lambda_1 = 3(X_1 - Z_1^2)(X_1 + Z_1^2)$, 因此计算 λ_1 只需要 $1M+1S$, 两倍点运算的计算量为 $4M+4S$.

(2) 特征 $p=2$ 的情形. 椭圆曲线的方程如 (19.2) 所示.

仿射坐标: 设 $P=(x_1,y_1)$, $Q=(x_2,y_2)$, $R=(x_3,y_3)=P+Q$. 如果 $P \neq Q$, 则有如下的加法计算公式:

$$\lambda = \frac{y_1+y_2}{x_1+x_2},$$
$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a,$$
$$y_3 = (x_1+x_3)\lambda + x_3 + y_1.$$

如果 $P=Q$, 则有下面的两倍加的计算公式:

$$\lambda = \frac{y_1}{x_1} + x_1,$$
$$x_3 = \lambda^2 + \lambda + a,$$
$$y_3 = (x_1+x_3)\lambda + x_3 + y_1.$$

因此, 在仿射坐标下, 椭圆曲线点的加法和两倍加的计算量都为 $2M+1S+1I$.

Jacobi 坐标: 令 $x = X/Z^2$, $y = Y/Z^3$, 则椭圆曲线的方程为

$$Y^2 + XYZ = X^3 + aX^2Z^2 + bZ^6.$$

令 $P=(X_1,Y_1,Z_1)$, $Q=(X_2,Y_2,Z_2)$, $R=(X_3,Y_3,Z_3)=P+Q$, 如果 $P \neq Q$, 采用 P1363 中的算法如下:

$$\begin{aligned}
\lambda_1 &= X_1Z_2^2, && 1M+1S,\\
\lambda_2 &= X_2Z_1^2, && 1M+1S,\\
\lambda_3 &= \lambda_1+\lambda_2, &&\\
\lambda_4 &= Y_1Z_2^3, && 2M,\\
\lambda_5 &= Y_2Z_1^3, && 2M,\\
\lambda_6 &= \lambda_4+\lambda_5, &&\\
\lambda_7 &= Z_1\lambda_3, && 1M,\\
\lambda_8 &= \lambda_6X_2+\lambda_7Y_2, && 2M,\\
Z_3 &= \lambda_7Z_2, && 1M,\\
\lambda_9 &= \lambda_6+Z_3, &&\\
X_3 &= aZ_3^2+\lambda_6\lambda_9+\lambda_3^3, && 3M+2S,\\
Y_3 &= \lambda_9X_3+\lambda_8\lambda_7^2, && 2M+1S.
\end{aligned}$$

因此, 在 Jacobi 坐标下, 加法的计算量是 $15M + 5S$, 如果 $Z_2 = 1$, 则对于 Jacobi 点的加法运算的计算量是 $11M + 4S$; 再进一步, 如果 $a = 0$, 则加法的计算量为 $10M + 3S$.

如果 $P = Q$, 则有下面的两倍加的计算公式:

$$\begin{aligned} Z_3 &= X_1 Z_2^2, && 1M + 1S, \\ X_3 &= (X_1 + dZ_1^2)^4, && 1M + 2S, \\ \lambda &= Z_3 + X_1^2 + Y_1 Z_1, && 1M + 1S, \\ Y_3 &= X_1^4 Z_3 + \lambda X_3, && 2M + 1S, \end{aligned}$$

其中 $d = b^{2^{n-2}}$, 可以预先计算出来. 因此, 在 Jacobi 坐标下, 特征 2 的椭圆曲线上点的两倍加的计算量为 $5M + 5S$.

§19.3 椭圆曲线的倍点运算

本节介绍常用的椭圆曲线倍点运算的方法, 这些算法对于特征 $p > 3$ 和特征 $p = 2$ 的椭圆曲线都适用, 并分析每个算法的运算效率. 为了方便, 称做一次椭圆曲线点的加法或两倍点运算为一次椭圆曲线运算.

为了方便, 用 n 表示有限域的大小 (比特数), 且倍点运算中的 k 与有限域的尺寸大小相当, 即 $\log k \sim n$.

一、二进制法

计算倍点运算的最常用方法是二进制法, 算法如下:

(算法 19.5) 倍点运算的二进制法

输入: 椭圆曲线上的点 P 及二进制整数 $k = \sum_{j=0}^{l-1} k_j 2^j$, $k_j \in \{0, 1\}$.

输出: 椭圆曲线上的点 $Q = [k]P$.

Step 1. 令 $Q = P$;

Step 2. For i from $l - 1$ to 1 do

$Q = 2Q$;

如果 $n_i = 1$, 则利用上一节的算法计算 $Q = Q + P$;

Step 3. 输出 Q.

这是最常用的算法, 在该算法中, 需要计算 $\log |k|$ 次两倍点运算和平均 $\frac{1}{2}\log(|n|)$ 次点的加法运算, 因此共需要 $\frac{3}{2}n$ 次椭圆曲线的运算.

二、m-ary 法

设 $m=2^r, r\geqslant 1$, 将 k 表示为 m 进制, 对于 $1\leqslant i<2^r$, 预计算 $[i]P$, 然后用类似上面二进制的方法进行计算. 而上面提到的二进制法实际上是 $r=1$ 的特殊情形.

(算法 19.6) 倍点运算的m-ary 算法

输入: 椭圆曲线上的点 P 及二进制整数

$$k=\sum_{j=0}^{d-1}k_jm^j,\quad k_j\in\{0,1,\cdots,m-1\}.$$

输出: 椭圆曲线上的点 $Q=[k]P$.

预计算:

Step 1. 令 $P_1=P$;

Step 2. For $i=2$ to $m-1$ 计算 $P_i=P_{i-1}+P$;

Step 3. $Q=\mathcal{O}$;

主循环

Step 4. For i from $d-1$ to 0 do

$Q=[m]Q$ (做 r 次两倍点运算);

$Q=Q+P_{k_j}$;

Step 5. 输出 Q.

在该算法中, 需要 $(d-1)r$ 个两倍点运算 (其中 $d=\lceil l/r\rceil$, 而 l 是 k 的二进制长度, 当然有 $l\sim n$), 需要 $W-1$ 次点的加法运算 (这里 W 是 $k_0,k_1,\cdots,k_{d-1}$ 中非零个数), 而预计算需要 2^r-2 次椭圆曲线的运算, 因此本算法共需要 $(d-1)r+W+2^r-3$ 个椭圆曲线的运算. 那么, 适当选择 m 的大小, 可以减少点的加法运算.

在主循环的第 1 步中, 如果将 $[m]Q$ 的计算分成两步进行, 则可以在预计算中减少一半的计算量, 这就是下面的改进后的 m-ary 法.

(算法 19.7) 倍点运算的改进m-ary 算法

输入: 椭圆曲线上的点 P 及二进制整数

$$k=\sum_{j=0}^{d-1}k_jm^j, k_j\in\{0,1,\cdots,m-1\}.$$

输出: 椭圆曲线上的点 $Q=[k]P$.

预计算:

Step 1. 令 $P_1 = P$; $P_2 = [2]P$.

Step 2. For $i = 2$ to $(m-2)/2$ 计算 $P_{2i+1} = P_{2i-1} + P_2$.

Step 3. $Q = \mathcal{O}$;

主循环

Step 4. For i from $d-1$ to 0 do

　　If $k_j \neq 0$, then do

　　　　Let $k_j = 2^{s_j} h_j$, 而 h_j 是奇数

　　　　$Q = [2^{r-s_j}]Q$,

　　　　$Q = Q + P_{h_j}$,

　　Else $s_j = r$.

　　$Q = [2^{s_j}]Q$;

Step 5. 输出 Q.

在该算法中, 预计算需要 1 次两倍点运算和 $2^{r-1}-1$ 次点的加法, 共 2^{r-1} 次椭圆曲线的运算. 在主循环中, 最多有 $l-1$ $(\sim n-1)$ 个两倍点的运算, 为了方便, 假定对任意的 $0 \leqslant j \leqslant d-1$, 都有 $k_j \neq 0$, 则主循环中需要 $d-1$ 个点的加法运算, 则该算法的计算量为

$$N(n,r) = 2^{r-1} + (n-1) + (d-1) = 2^{r-1} + n + \frac{n}{r} - 2.$$

求极值得, 当 $r = \log_2 n - (2 - o(1)) \log_2 \log_2(n)$ 时, 该算法所需要的椭圆曲线的运算 $N(n,r)$ 达到最小.

例 19.7 设椭圆曲线的基域为 $\mathbb{F}_p$, 其中 p 是 192 比特的素数, 即 $n = 192$, 对不同的 r, 计算 $N(n,r)$, 如下表所示:

r	1	2	3	4	5	6
$N(n,r)$	$288^{(*)}$	288	258	246	245	254

其中 $(*)$ 表示用通常的二进制法所需要的计算量. 由上表可知, 当 r 取 5 时比较合适, 此时椭圆曲线的倍点运算所需要的椭圆曲线运算量由平均 288 次减少到平均 245 次.

例 19.8 设 $k = 4997505654740941634156403062595398316589553260676595800838$ 为一整数.

(1) 二进制法：k 的二进制表示为

110010111101000001100100110000001010001001100010010001010111010011010
001011010110011000111101010111111111011100110111010111110110111010101

$$111001110000000011101110110010101000011010110110000110,$$

它的重量为 $W = 100$, $\log_2 k = 192$, 因此在普通的二进制法中, 需要 191 个两倍加运算和 99 个点的加法, 因此共需要 290 个椭圆曲线计算.

(2) m-ary 法：取 $m = 2^5$, 则 k 的 m 进制表示为

$$\underline{11}, \underline{00101}, \underline{11101}, \underline{00000}, \underline{11001}, \underline{00110}, \underline{00000}, \underline{10100}, \underline{01001}, \underline{10001}, \underline{00100}, \underline{01010},$$

$$\underline{11101}, \underline{00110}, \underline{10001}, \underline{01101}, \underline{01100}, \underline{11000}, \underline{11110}, \underline{10101}, \underline{11111}, \underline{11101}, \underline{11001}, \underline{10111},$$

$$\underline{01011}, \underline{11101}, \underline{10111}, \underline{01010}, \underline{11110}, \underline{01110}, \underline{00000}, \underline{01110}, \underline{11101}, \underline{10010}, \underline{10100}, \underline{00110},$$

$$\underline{10110}, \underline{11000}, \underline{00110},$$

其重量为 $W = 36$, 因此在 m-ary 算法中, 预计算需要 30 个椭圆曲线运算, 而主循环中需要 $38 * 5 = 190$ 个两倍加运算和 $W - 1 = 35$ 个椭圆曲线点的加法运算, 因此共需要 $30 + 35 + 190 = 255$ 个椭圆曲线运算. 此时诸 k_i 为

i	0	1	2	3	4	5	6	7	8	9	10	11	12
k_i	6	24	22	6	20	18	29	14	0	14	30	10	23
i	13	14	15	16	17	18	19	20	21	22	23	24	25
k_i	29	11	23	25	29	31	21	30	24	12	13	17	6
i	26	27	28	29	30	31	32	33	34	35	36	37	38
k_i	29	10	4	17	9	20	0	6	25	0	29	5	3

(3) 改进 m-ary 算法：和普通的 m-ary 算法相比, 只是在预计算时, 由原来的 30 个椭圆曲线运算减少到 $2^4 - 1 = 15$ 个椭圆曲线运算, 因此整个 $[k]P$ 的倍点运算需要 $255 - 15 = 240$ 个椭圆曲线运算. 此时, 诸 k_i 的值如下表所示：

i	0	1	2	3	4	5	6	7	8	9	10	11	12
k_i	3	3	11	3	5	9	29	7	0	7	15	5	23
i	13	14	15	16	17	18	19	20	21	22	23	24	25
k_i	29	11	23	25	29	31	21	15	3	3	13	17	3
i	26	27	28	29	30	31	32	33	34	35	36	37	38
k_i	29	5	1	17	9	5	0	3	25	0	29	5	3

三、窗口法

在上面改进的 m-ary 算法中, 在计算 $k_j = 2^{s_j} h_j$ 时, 进行移位运算, 这就使得 h_j 没有充分用到高位的比特值, 因而预计算的利用率不高 (即用到的大多数是比较小的 $[i]P$), 下面的方法解决了这一缺点. 这种方法的想法如下：如果比特值为 0, 则直接跳过 (实际上是进行一次倍点运算), 如果比特值为 1, 则取一整数段 (r 个比特). 算法如下：

(算法 19.8) 倍点运算的滑动窗口算法

输入：椭圆曲线上的一点 P 及二进制整数 $k=\sum_{j=0}^{l-1}k_jm^j$, $k_j\in\{0,1\}$.

输出：椭圆曲线上的点 $Q=[k]P$.

预计算:

1. 令 $P_1=P$; $P_2=[2]P$;
2. For $i=1$ to $2^{r-1}-1$ 计算 $P_{2i+1}=P_{2i-1}+P_2$;
3. $Q=\mathcal{O}$, $j=l-1$;

主循环

4. While $j\geqslant 0$ do

    If $k_j=0$, then $Q=[2]Q$, $j=j-1$;

    Else do

        取最小的 t 满足 $j-t+1\leqslant r$ 且 $k_t=1$,

        $h_j=(k_jk_{j-1}\cdots k_t)_2$, (二进制表示)

        $Q=[2^{j-t+1}]Q+P_{h_j}$,

        $j=t-1$;

5. 输出 Q.

在 m-ary 法中, 由于每次都处理 s ($s\leqslant r$) 个比特, 如果将这 s 个比特看作 "窗口", 则 m-ary 法就是 "固定窗口法", 而上面的方法称为 "滑动窗口法". 也就是说, 如果比特值为 0, 就将 "窗口" (r 个比特) 滑过去. 从直观上看, "滑动窗口" 的效果相当于固定窗口, 而窗口的宽度增加了一个比特 (上面的 m-ary 法中 $m=2^{r+1}$), 而预计算是一样的, 这就减少了椭圆曲线点的加法的次数. 类似于 m-ary 算法的分析, 可知该算法的椭圆曲线运算的计算量为

$$N(n,r)=2^{r-1}+(n-1)+(d-1)=2^{r-1}+n+\frac{n}{r+1}-2.$$

注：同 m-ary 算法相比, 在 "滑动窗口法" 算法中, 椭圆曲线两倍点的运算没有减少, 所减少的只是椭圆曲线点的加法.

例 19.9 设 k 如例 19.8 中所示, 则在 "滑动窗口法" 算法中的诸窗口表示如下：

$\underline{11001},0,\underline{1111},0,\underline{1},00000,\underline{11001},00,\underline{11},000000,\underline{101},000,\underline{10011},000,\underline{1001},000,$

$\underline{10101},\underline{1101},00,\underline{1101},000,\underline{1011},0,\underline{1011},00,\underline{11},000,\underline{1111},0,\underline{10101},\underline{11111},\underline{11101},$

$\underline{11001},\underline{10111},0,\underline{10111},\underline{11011},0,\underline{11101},0,\underline{10111},\underline{10011},\underline{1},0000000,\underline{11101},\underline{11011},$

$$00,\underline{10101},0000,\underline{1101},0,\underline{11011},00000,\underline{11},0.$$

可知窗口有 $W=32$ 个, 因此需要 $W-1=31$ 个椭圆曲线点的加法; 预计算仍然是 $2^4-1=15$ 个椭圆曲线运算, 而两倍点的运算需要 191 个, 因此总的计算量为 $191+31+15=237$ 个椭圆曲线运算.

四、NAF 法

在椭圆曲线点的运算中, 点的减法和加法的计算效率一样. 如果基域的特征大于 2, 点 $P=(x,y)$ 是椭圆曲线上一点, 则 $-P=(x,-y)$; 如果基域的特征为 2, 点 $P=(x,y)$ 是椭圆曲线上一点, 则 $-P=(x,x+y)$. 因此, 如果在 k 的表达式中有 ±1, 那么在椭圆曲线的倍点运算中, 将可能减少点的加法运算.

设整数 k 是 l 比特长, 则可以将 k 写成形如 $\sum_{j=0}^{l} s_j 2^j$, 其中 $s_j\in\{-1,0,1\}$, 称这种形式为带符号的二进制表示, 简记为 SD 表达式 (binary signed digit representation). 由于这种形式一共有 3^{l+1} 个, 而 l 比特的整数只有 2^l 个数, 因此这种表示形式不是惟一的, 例如 $7=(0111)_2=(100\bar{1})_2$, 这里 $\bar{1}=-1$. 但是如果要求该表达式是稀疏的, 即在该表达式中, 没有任何两个非零的值相邻, 也就是说对任意的 $j\geqslant 0$, 有 $s_js_{j+1}=0$, 这种表示形式称为 NAF (non-adjacent form). 下面的定理表明整数的 NAF 形式有利于减少椭圆曲线倍点运算的计算量.

定理 19.2　*每一个整数 k 有惟一的NAF表达式; 在 k 的所有SD表达式中, NAF表达式的重量最小; NAF表达式的比特长度比二进制的比特长度最多长一个比特.*

证明可参阅文献 [24,77,78] 等.

计算 NAF 表达式的思想和计算二进制表达式的方法一样: 不断地用 2 除, 保存余数, 再对商用 2 除, 一直进行下去就得到整数的二进制表达式. 为了得到 NAF 表达式, 也不断地用 2 除, 对余数选择 $\{0,\pm1\}$, 保证商是偶数, 再对商用 2 除, 一直进行下去, 就可以得到整数的 NAF 表达式. 下面是具体的算法计算整数 k 的 NAF 表达式:

(算法 19.9)　转换为 NAF 表达式

输入: 整数 k.

输出: NAF 表达式 $k=\sum_{j=0}^{l} s_j 2^j$, $s_j\in\{-1,0,1\}$.

Step 1. $j=0$;

Step 2. while $k>0$ do

　　　　if k 是奇数,

　　　　　　$s_j=2-(k \bmod 4)$;

　　　else

　　　　　$s_j = 0;$

　　　$k = (k - s_j)/2;$

　　　$j = j + 1;$

Step 3. 输出 $(s_l s_{l-1} \cdots s_0)$.

上述算法用到了大整数加 1 的运算, 不太方便, 可以对其进行适当的改造, 使得只处理每一位上的运算, 下面的 NAF 算法取自 [74]:

(算法 19.10)　倍点运算的 NAF 算法

输入: 整数 k 及椭圆曲线上一点 P.

输出: 倍点 $[k]P$.

Step 1. 令 $h_l h_{l-1} \cdots h_1 h_0$ 是 $3k$ 的二进制表达式, 其中 $h_l = 1$;

Step 2. 令 $k_l k_{l-1} \cdots k_1 k_0$ 是 k 的二进制表达式;

Step 3. 令 $S = P$;

Step 4. for i from $l-1$ to 0 do

　　　$S = [2]S;$

　　　if $h_i = 1$ 且 $k_i = 0$

　　　　　计算 $S = S + P;$

　　　if $h_i = 0$ 且 $k_i = 1$

　　　　　$S = S - P;$

Step 5. 输出 S.

可以证明, 整数的 NAF 表达式的重量平均为 $\frac{1}{3}\log_2 k$ (可以参阅文献 [24]). 因此在 NAF 算法中, 需要 $n-1$ 个倍点运算和平均 $\frac{1}{3}n$ 个点的加法, 共 $\frac{4}{3}n$ 个椭圆曲线的运算.

例 19.10　设 k 如例 19.8 中所示, 则 k 的 NAF 表达式为

$$10\bar{1}010\bar{1}000\bar{1}01000010\bar{1}001010\bar{1}0000001010001010\bar{1}00010010010\bar{1}0\bar{1}00\bar{1}01010\bar{1}0100$$

$$10\bar{1}00\bar{1}0\bar{1}0\bar{1}010\bar{1}0010000\bar{1}0\bar{1}0\bar{1}000000000\bar{1}00\bar{1}0100\bar{1}000\bar{1}0\bar{1}00000\bar{1}00\bar{1}000\bar{1}0\bar{1}0\bar{1}000\bar{1}$$

$$0100\bar{1}00000001000\bar{1}000\bar{1}0\bar{1}0010101000100\bar{1}0\bar{1}00\bar{1}0\bar{1}000010\bar{1}0$$

(其中 $\bar{1} = -1$), 其重量为 $W = 65$, 因此在 NAF 算法中, 需要 $192 - 1 = 191$ 个两倍点运算和 $W - 1 = 64$ 个点的加法运算, 总的计算量为 $191 + 64 = 255$ 个椭圆曲线运算.

例 19.8 和 19.10 表明：NAF 算法优于通常二进制法, 和 m-ary 的算法相当.

事实上, 我们还可以很自然地将 NAF 表达式与 m-ary 法、滑动窗口法结合起来, 进一步减少椭圆曲线点的加法的次数. 这些方法都很简单, 也很直观, 限于篇幅, 这里从略.

五、查表法

在椭圆曲线公钥密码算法中, 例如在 P1363[74] 所推荐的数字签名算法和加密算法, 都有一个固定点的倍点运算, 即基点 P 的倍点运算. 对于这个倍点运算, 可以在系统初始化时, 预先计算出所有的 $[2]P, [2^2]P, \cdots, [2^n]P$, 存储起来, 得到如下基于 NAF 的查表法倍点运算：

(算法 19.11)　倍点运算的查表法

输入：整数 k 的 NAF 表达式 $\sum_{j=0}^{n-1} s_j 2^j$, $s_j \in \{0, 1, -1\}$.

输出：椭圆曲线上的点 $Q = [k]P$.

预计算:

Step 1. 令 $P_1 = P$;.

Step 2. For $i = 1$ to $n-1$ 计算 $P_{2^i} = [2]P_{2^{i-1}}$.

Step 3. $Q = \mathcal{O}$;

主循环

Step 4. for i from 0 to $n-1$

　　If $s_i = 1$, then $Q = P_{2^i} + P$;

　　If $s_i = -1$, then $Q = P_{2^i} - P$;

Step 5. 输出 Q.

与前面的算法相比, 这个算法中省去了所有的两倍点的运算, 只需要平均 $n/3$ 个椭圆曲线的运算.

§19.4　Frobenius 展开

这一节, 我们先考虑有限域 $\mathbb{F}_2$ 上的椭圆曲线

$$E_0: \quad y^2 + xy = x^3 + 1 \tag{19.3}$$

和

$$E_1: \quad y^2 + xy = x^3 + x^2 + 1. \tag{19.4}$$

直接计算可知 $E_1(\mathbb{F}_2)$ 上有 2 个点: $\{\mathcal{O},(0,1)\}$, 而 $E_0(\mathbb{F}_2)$ 上有 4 个点: $\{\mathcal{O},(0,1),(1,0),(1,1)\}$. 设 t_a 为 Frobenius 变换

$$\begin{array}{rccc}\phi: & E_a(\mathbb{F}_2) & \longrightarrow & E_a(\mathbb{F}_2),\\ & (x,y) & \longmapsto & (x^2,y^2)\end{array}$$

的迹, 则有

$$\#E_a(\mathbb{F}_2)=2+1-t_a,\quad a=0,1.$$

因此 $t_0=-1$, $t_1=1$, 称这样的椭圆曲线为反常椭圆曲线 (anomalous). 易知 ϕ 满足方程

$$\phi^2-t\phi+\mathcal{Q}=0,$$

其中 $t=\mathcal{Q}+1-\#E(\mathbb{F}_q)$ 称为 Frobenius 变换 ϕ 的迹. 在复数域中, 则 $\phi=\frac{t+\sqrt{-7}}{2}\notin\mathbb{Z}$, 称这样的椭圆曲线具有复乘. 考虑整环 $\mathbb{Z}[\phi]=\{a+b\phi|a,b\in\mathbb{Z}\}$, 则易知 $\mathbb{Z}[\phi]$ 是 Euclid 整环. 令 $E_a(\mathbb{F}_{2^n})$ 表示由方程 (19.3) 和 (19.4) 定义的在基域 $\mathbb{F}_{2^n}$ 上的椭圆曲线. 如果有限域 $\mathbb{F}_{2^n}$ 采用正规基表示, 则 Frobenius 变换的计算是容易的

$$\phi(x,y)=(x^2,y^2),\ \phi^2(x,y)=(x^{2^2},y^{2^2}),\ \cdots,\ \phi^{2^k}=(x^{2^k},y^{2^k}).$$

这是因为在有限域的正规基表示中, x^{2^k} 的计算实际上是移位运算, 因此计算速度很快.

在倍点运算 $[k]P$ 中, 将 k 看作 $\mathbb{Z}[\phi]$ 中的元素, 如果能够将 k 写成如下形式:

$$k=a_0+a_1\phi+a_2\phi^2+\cdots+a_s\phi^s,\quad a_i\in\{0,1\}.\tag{19.5}$$

令 W 表示 (19.5) 式中非零 a_i 的个数, 则计算 $[k]P$ 实际上只需要 W 个椭圆曲线点的加法运算.

下面研究如何计算表达式 (19.5), 首先有

定理 19.3 *$a+b\phi$ 能被 ϕ 整除的充分必要条件是 a 为偶数.*

证明 如果 $a+b\phi$ 能被 ϕ 整除, 则存在 $u+v\phi\in\mathbb{Z}[\phi]$, 使得

$$a+b\phi=(u+v\phi)\phi=-2v+(u+tv)\phi,$$

因而 $a=-2v$ 是偶数. 反之, 若 $a=2v$ 是偶数, 则

$$a+b\phi=2v+b\phi=(t\phi-\phi^2)v+b\phi=((tv+b)-v\phi)\phi,\tag{19.6}$$

因此 $a+b\phi$ 是 ϕ 的倍数.

上面的定理说明, 对于任意的 $a+b\phi\in\mathbb{Z}[\phi]$, ϕ 除 $a+b\phi$ 的余数为 0 或 1 (计算商的公式如 (19.6) 式). 不断地用 ϕ 除, 便可得到表达式 (19.5).

例 19.11　考虑椭圆曲线 (19.4), 计算 9 的 ϕ 表达式.

解　此时 $t=1$, ϕ 满足方程 $\phi^2-\phi+2=0$, 则

$$\begin{aligned}9&=1+2\cdot 4=1+(\phi-\phi^2)4=1+\phi(4-4\phi)\\&=1+\phi(2(\phi-\phi^2)-4\phi)=1+\phi^2(-2-2\phi)\\&=1+\phi^2((\phi^2-\phi)-2\phi)=1+\phi^3(-3+\phi)\\&=1+\phi^3+\phi^3(-4+\phi)=1+\phi^3+\phi^3(-2(\phi-\phi^2)+\phi)\\&=1+\phi^3+\phi^4(-1+2\phi^2)=1+\phi^3+\phi^4+\phi^4(-2+2\phi)\\&=1+\phi^3+\phi^4(-(\phi-\phi^2)+2\phi)=1+\phi^3+\phi^4+\phi^5(1+\phi)\\&=1+\phi^3+\phi^4+\phi^5+\phi^6.\end{aligned}$$

NAF 的方法也可以照搬过来, 为此, 对于任意的 $a+b\phi\in\mathbb{Z}[\phi]$, 定义 $a+b\phi$ 的范数为

$$N(a+b\phi)=(a+b\phi)(a+b\overline{\phi})=a^2+tab+2b^2,$$

而 ϕ 的范数 $N(\phi)=2$.

为了得到 ϕ 的 NAF 表达式, 类似于前面整数的情形, 不断地用 ϕ 除, 由于 $N(\phi)=2$, 因此余数为 $\{0,\pm 1\}$, 选择合适的余数, 使得商能够被 ϕ 整数 (如前所述, 只要商的实部为偶数即可). 一直对商用 ϕ 除, 最后就可以得到所需要的 NAF 表达式. 因此有如下的算法:

(算法 19.12)　计算 Frobenius 表达式

输入: $x_0+y_0\phi\in\mathbb{Z}[\phi]$.

输出: ϕ-adic NAF 表达式.

Step 1. $x=x_0, y=y_0$;

Step 2. $S=\emptyset$;

Step 3. While $x\neq 0$, 或者 $y\neq 0$,

　　如果 x 是奇数, 令 $u=2-(x-2y \bmod 4)$;

　　否则令 $u=0$;

　　$x=x-u$;

　　将 u 添加到 S 中的前面;

　　$(x,y)=(y+(xt)/2,-x/2)$;

Step 4. 输出 S.

例 19.12 考虑椭圆曲线 (19.4), 计算 9 的 ϕ-adic NAF 表达式.

解 此时 $t=1$, ϕ 满足方程 $\phi^2-\phi+2=0$, 则

$$\begin{aligned}9&=1+8=1+\phi(4-4\phi) \quad /*u=1*/\\&=1+\phi^2(-2-2\phi) \quad /*u=0*/\\&=1+\phi^3(-3+\phi) \quad /*u=0*/\\&=1-\phi^3+\phi^3(-2+\phi) \quad /*u=-1*/\\&=1-\phi^3+\phi^3(\phi^2-\phi+\phi)=1-\phi^3+\phi^5.\end{aligned}$$

注意, 在进行倍点运算 $[k]P$ 时, 因为 $N(k)=k^2$, $N(\phi)=2$, 而每次除 ϕ 时, 范数少一半, 因此 k 的 ϕ-adic NAF 表达式的长度是 k 的二进制长度的两倍, 这是和整数的 NAF 表达式相比的缺点. 但是这一点可由下面的方法来弥补：注意到

$$\phi^n(P)=P$$

(注意, 使用的有限域是 $\mathbb{F}_{2^n}$), 也就是说 $\phi^n=1$, 而 $N(\phi^n)=2^n$, 因此在进行倍点运算之前, 先计算 $k \pmod{\phi^n}$, 再计算 ϕ-adic 的 NAF 表达式, 就可以保证其 ϕ-adic NAF 表达式的长度与 n 相当.

为此首先要计算 $\phi^n-1=x+y\phi$, 这可重复利用

$$\phi^2-t\phi+2=0$$

来得到, 而且这个过程在系统初始化时, 预先计算出来.

再计算 $\phi^n-1=x+y\phi$ 除 k 的余数 $m+n\phi$, 这可由如下公式得到：

$$\frac{k}{x+y\phi}=\frac{k(x+y\overline{\phi})}{(x+y\phi)(x+y\overline{\phi})}=\frac{(k(x+yt))-ky\phi}{x^2+txy+2y^2}.$$

取 m 为 $k(x+yt)$ 除以 $x^2+txy+2y^2$ 的最小非负余数, n 为 $-k$ 除以 $x^2+txy+2y^2$ 的最小非负余数, 则 $m+n\phi$ 为所求.

可以证明, 经过如上处理后, 所得到的 ϕ-adic NAF 表达式的重量平均为 $n/3$, 具体证明可参阅文献 [79]. 这样在椭圆曲线的倍点运算中, 只需要 $n/3$ 个点的加法运算, 而不需要两倍加运算. 因此这个算法的效率相当于特征 $p>3$ 时, 带 NAF 的查表法的效率. 但对于特征 $p>3$ 的情形, 带 NAF 的查表法只能适用固定点的倍点运算, 而目前这个算法对于特征 $p=2$ 的椭圆曲线上任一点的倍点运算都适合.

移动窗口的方法也可以移植到 ϕ-adic NAF 表达式的情形, 以进一步减少椭圆曲线点的加法运算, 细节简单, 这里从略.

上述方法可以推广到 $\mathbb{F}_{2^d}$, 其中 d 比较小的情形, 也可以推广到小特征域 $\mathbb{F}_{q^n}$, 其中 q 是小素数的情形, 这可参阅文献 [80].

参考文献

1 Mao W. Modern Cryptography: Theory and Practice, 2003

2 Dutta R, Barua R, Sarkar P. Pairing-Based Cryptography : A Survey, Cryptology ePrint Archive, Report 2004/064

3 Galbraith S D. Supersingular curves in cryptography, Advances in Cryptology-Asiacrypt'2001, Lecture Notes on Computer Science 2248, Springer-Verlag 2002, 495~513

4 Joux A. A one-round protocol for tripartite Diffie-Hellman, Algorithm Number Theory Symposium-ANTS-IV, Lecture Notes on Computer Science 1838, Springer-Verlag 2000, 385~394

5 Choi K Y, Hwang J Y, Lee D H. Efficient ID-based Group Key Agreement with Bilinear Maps, Practice and Theory in Public Key Cryptography-PKC'2004. Singapore(SG), March 2004. In: Lecture Notes on Computer Science Vol 2947. New York:Springer-Verlag 2004, 130~144

6 Boneh D, Franklin M. Identity-based encryption from the Weil pairing, Advances in Cryptology-Crypto'2001, Lecture Notes on Computer Science 2139, Springer-Verlag 2001, 213~229

7 Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing. In: Proceedings of Asiacrypt, 2001

8 Cha, Jae Choon and Cheon, Jung Hee, An Identity-Based Signature from Gap Diffie-Hellman Groups. In: Lecture Notes in Computer Science vol 2567. New York: Springer-Verlage, 2002. 18~30

9 Libert B, Quisquater J J. New Identity Based Signcryption Schemes from Pairings. Cryptology ePrint Archive, Report 2003/023

10 裴定一, 模形式和三元二次型, 上海科技出版社, 1994

11 Serge Lang, Elliptic Functions, Addison–Wesley, 1973.

12 Silverman J H. The arithmetic of elliptic curves, Volume 106 of Graduate Texts in Mathematics, Springe-Verlag, 1986

13 Vèlu J. Isogenies entre courbes elliptiques. C R Acad Sci Paris Sèr I Math, Ser A, 1971, 273:238~241

14 Hartshorne R. Algebraic geometry, Springer-Verlag, 1977

15 Shafarevich I R. Basic algebraic geometry, Springer-Verlag, 1977

16 Schoof R. Elliptic curves over finite fields and the computation of square roots mod p. Math. Comp., 1985, 44: 483~494

17 Rosenberger G, Wang X. Some properties of reduced modular polynomials, Results in Mathematics, 2002, 42: 349~358

18 Schoof R. Counting points on elliptic curves over finite fields, Journal de Theorie des Nombres de Bordeaux 1995, 7: 219~254

19 Müller V. Ein Algorighmus zur Bestimmung der Punttanzahl elliptischer Kurren über endlichen Körpern der charakteristik grþer drei. Ph. D. Thesis, Universität des Saarlandes,

1995

20 Cassels. Lecture on Elliptic Curves. Cambridge: Cambridge University Press,1991

21 Gaudry, A Comparison and a Combination of SST and AGM algorithms for Counting Points of Elliptic Cruves in Characteristic 2. Advances in Cryptology, Asiacrypt'2002, Springer-Verlag, LNCS 2501, 2002, 311~327

22 伍鸿熙等, 紧黎曼曲面引论, 科学出版社.

23 Cohen H, Miyaji A, Ono T. Efficient elliptic curve exponentiation using mixed coordinates. Advances in Cryptology-Asiacrypt'98. In: LNCS Vol 1514, New York: Springer-Verlag, 1998, 51~56

24 Morain F, Olivos J. Speeding up the computations on an elliptic curve using addition-subtraction chains, Info. Theory Appl., 1990, 24: 531~543

25 Blake Ian. Gadiel Seroussi and Nigel Smart, Elliptic Curves in Cryptography. Cambridge: Cambridge Univ. Press, 1999

26 Pollard J M. Monte Carlo methods for index computation (mod p), Math. of Computation, 1978, 32: 918~924

27 Pohlig S, Hellman M. An improved algorithm for computing logarithm over $GF(p)$ and the cryptographic significance. IEEE Trans. Inform. Theory 1978, 24: 106~110

28 Menezes A T, Okamoto T, Vanstone S A. Reducing elliptic curve logarithms in a finite field. IEEE Trans. Inform. Theory, 1993, 39: 1639~1646

29 Schoof R. Nonsingular plane cubic curves over finite fields, J. of Combinatorial Theory, Series A, 1987, 46: 183~211

30 Frey G, Müller M, Rück H. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans. Theory, 1999, 45: 1717~1719

31 Frey G, Rück H. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math. of Computation, 1994, 62: 865~874

32 Lichtenbaum S. Duality theorems for curves over $p-adic$ fields, Invent. Math. 1969, 7: 120~136

33 Balasubramanian R, Koblitz N. The impobability that an elliptic curve has subexponential discrete log problem under the Menezes-Okamoto-Vanstone algorithm. J of Cryptology, 1998, 11: 141~145

34 Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves, Comm. Math. Univ. Sancti Pauli, 1998, 47: 81~92

35 Semaev I. Evaluation of discrete logarithms in a group of $p-$torsion points of an elliptic curve in characteristic p, Maht. of Computation, 1998, 67: 353~356

36 Smart N P. The discrete logarithm problem of elliptic curves of trace one, preprint. 1997

37 祝跃飞, 裴定一, 异常椭圆曲线上的 DLP 的一个算法, 中国科学 (A 辑), 2001, 31: 332~336

38 Canfield E R, Erodös P, Pomerance C. On a problem of Oppenheim concerning factorization numerorum, J Number Theory, 1983, 17: 1~28

39 Hellman M E, Reyneri J M. Fast computation of discrete logarithms in $GF(q)$, Advances in Cryptography: Proceedings of CRYPTO'82. D.Chaum, R.Rivest and A.Sherman eds., Plenum Press, 1983, 3~13

40 Berlekamp E R. Algebraic Coding Theory. New York: McGraw Hill, 1978

41 Lidl R, Niederreiter H. Finite fields, Addison–Wesley Publishing Company 1983

42 Gordon D. Discrete logarithms in GF(p) using the number field sieve, SIAM J. Discrete Math., 1993, 6: 312~323

43 Schirokauer O. Discrete logarithms and local units, Phil. Trans. R. Soc. Lond. 1993, A 345: 409~423

44 Adelman L M. The function field sieve. In: Algorithmic Number Theory. LNCS877, 1994, 108~121

45 Coppersith D. Fast evalution of logarithms in fields of characteristic. IEEE Transactions on Information Theory, 1984, 30: 587~594

46 Koblitz N. Hyperelliptic cryptosystems, J. of Cryptology, 1989, 1: 139~150

47 *Cantor D G. Computing in the Jacobian of hyperelliptic curve. Math of Computation, 1987,* 48: 95~101

48 Smart N P. On the performance of hyperelliptic cryptosystems, Eurocrypt'99, LNCS 1592, 165~175

49 LaMacchia B A, Odlyzko A M. Solving large sparse linear systems over finite fields, Advances in Crypto logy-Crypto'90, Springer-Verlag, LNCS 537, 1990, 109~133

50 Wiedemann D H. Solving sparse linear equations over finite fields, IEEE Trans. Inform. Theory, IT-32, no. 1986, 1: 54~62

51 Eberly W, Kaltofen E. On randomized Lanczos algorithms. In W.W.Küchlin editor, ISSAC97-Proceedings of the 1997 International Sympoblic and Algebraic Computation, ACM Press, 1997, 176~183

52 Pomerance C. Fast, Vigorous factorization and discrete logarithm algorithm. Discrete Algorithm and Complexity Proceedings of the Japan-US Joint Seminar, June 4–6, 1986, Kyoto, Japan, Perspectives in Computing, Pages Orlando, Academic Press. 1987, 119~143

53 Artin E. Quadratische Körper im Gebiete der hheren Kongruenzen I, II. Math Z, 1924, 19: 153~206

54 Paulus S, GRück H. Real and imaginary quadratic representations of hyperelliptic function fields, Math. of Comp., 1999, 68: 1233~1241

55 Bosch S, Lütkebohmert W, Raynaud W. Néron Models. Berlin: Springer-Verlag, 1980

56 Neukirch J. Algebraic Number Theory, Springer-Verlag, 1999

57 Stichtenoth H. Algebraic function fields and codes, Springer-Verlag, 1993

58 Chevalley C. Introduction to the theory of algebraic functions of an variable. In: Math Surveys Number VI. ASM, 1951

59 Huppert B. Endliche Gruppen, Springer-Verlag, Berlin, 1967

60 Lang S. Algebra (Third Edition), Addison-Wesleg Publishing Company 1993

61 Semaev I. Summation polynomials and discrete logarithm problem on elliptic curves, Preprint, 2004

62 Cohen H. A Course in Computational Algebraic Number Theory, GTM Vol 138. New York: Springer-Verlag, 1993

63 ElGamal T. *A subexponential algorithm for computing discrete logarithms over* $GF(p^2)$, IEEE Trans. Inform. Theory, vol. IT31 1985, 473~481

64 Advances in Cryptology-Eruocrypt' 98, International conference on the theory and application of cryptographic techniques, Espoo, Finland, May *31*-June *4, 1998*, Proceeding, volume *1403* of Lecture Notes in Computer Science, Springer-Verlag, 1998

65 Adleman L M, Demarrais J. A subexponential algorithm for discrete logarithms over all finite fields. Math of Computation, 1993, 61 (203): 1~15

66 Cohen H. Advanced Topics in Computational Number Theory. GTM Vol 193, New York: Springer-Verlag, 2000

67 Washington S C. Introduction to cyclotomic fields, vol. 83 of GTM, Springer-Verlag, 1982

68 Shimura, Abelian varieties with complex multiplication and modular functions, Princeton University Press, 1997

69 Hayes R D. Explicit class field theory in global function fields, stud. Alg. Number Th. / Adv. Math. Suppl. Stud., 1979, 6: 173~217

70 Roquetle P. Class field theory in Characteristic p, its origin and development, 1999

71 Adleman L M, Huang M A. Function field sieve method for discrete logarithms over finite fields. Information and computation, 1999, 151: 5~16

72 Tate, WC-groups over p-adic fields, Sem. Bourbaki, 156: 13p., December 1957

73 Maurer U, Wolf S. The relationship between breaking the Diffie-Hellman protocal and computing discrete logarithms. SIAM Journal on Computing, 1999, 28: 1689~1721

74 IEEE P1363/D3 (Draft version 3), specifications for public key cryptography, May 1998

75 Mullin R, Onyszchuk I, Vanstone S A, Wilson R. Optimal normal bases in $GF(p^n)$. Discrete Appl. Math., 1988, 22: 149~161

76 Itoh T, Tsufii S. A fast algorithm for computing multiplicative inverses in $GF(2^m)$ using normal bases. Info. and Comput., 1988, 78(3): 171~177

77 Clark W D, Liang J J. On arithmetic weight for a general radix representation of integers. IEEE Trans Info Theory, 1973, 19: 823~826

78 Reitwiesner G. Binary arithmetic. Adv. in Comp., 1960, 1: 231~308

79 Meier W, Staffelbach O. Efficients multiplication on certain non-supersingular elliptic curve, Proc. Crypto'92, Springer-Verlag, 1993, 333~344

80 Müller V. Fast multiplication on elliptic curves over small fields of characteristic two. J. Crypto., 1998, 11: 219~234

索　引

《现代数学基础丛书》已出版书目

(按出版时间排序)

1 数理逻辑基础（上册） 1981.1 胡世华、陆钟万 著
2 紧黎曼曲面引论 1981.3 伍鸿熙、吕以辇、陈志华 著
3 组合论（上册） 1981.10 柯召、魏万迪 著
4 数理统计引论 1981.11 陈希孺 著
5 多元统计分析引论 1982.6 张尧庭、方开泰 著
6 概率论基础 1982.8 严士健、王隽骧、刘秀芳 著
7 数理逻辑基础（下册） 1982.8 胡世华、陆钟万 著
8 有限群构造（上册） 1982.11 张远达 著
9 有限群构造（下册） 1982.12 张远达 著
10 环与代数 1983.3 刘绍学 著
11 测度论基础 1983.9 朱成熹 著
12 分析概率论 1984.4 胡迪鹤 著
13 巴拿赫空间引论 1984.8 定光桂 著
14 微分方程定性理论 1985.5 张芷芬、丁同仁、黄文灶、董镇喜 著
15 傅里叶积分算子理论及其应用 1985.9 仇庆久等 编
16 辛几何引论 1986.3 J.柯歇尔、邹异明 著
17 概率论基础和随机过程 1986.6 王寿仁 著
18 算子代数 1986.6 李炳仁 著
19 线性偏微分算子引论（上册） 1986.8 齐民友 著
20 实用微分几何引论 1986.11 苏步青等 著
21 微分动力系统原理 1987.2 张筑生 著
22 线性代数群表示导论（上册） 1987.2 曹锡华等 著
23 模型论基础 1987.8 王世强 著
24 递归论 1987.11 莫绍揆 著
25 有限群导引(上册) 1987.12 徐明曜 著
26 组合论（下册） 1987.12 柯召、魏万迪 著
27 拟共形映射及其在黎曼曲面论中的应用 1988.1 李忠 著
28 代数体函数与常微分方程 1988.2 何育赞 著

63 调和分析及其在偏微分方程中的应用 1999.10 苗长兴 著
64 惯性流形与近似惯性流形 2000.1 戴正德、郭柏灵 著
65 数学规划导论 2000.6 徐增堃 著
66 拓扑空间中的反例 2000.6 汪林、杨富春 编著
67 拓扑空间论 2000.7 高国士 著
68 非经典数理逻辑与近似推理 2000.9 王国俊 著
69 序半群引论 2001.1 谢祥云 著
70 动力系统的定性与分支理论 2001.2 罗定军、张祥、董梅芳 编著
71 随机分析学基础（第二版） 2001.3 黄志远 著
72 非线性动力系统分析引论 2001.9 盛昭瀚、马军海 著
73 高斯过程的样本轨道性质 2001.11 林正炎、陆传荣、张立新 著
74 数组合地图论 2001.11 刘彦佩 著
75 光滑映射的奇点理论 2002.1 李养成 著
76 动力系统的周期解与分支理论 2002.4 韩茂安 著
77 神经动力学模型方法和应用 2002.4 阮炯、顾凡及、蔡志杰 编著
78 同调论——代数拓扑之一 2002.7 沈信耀 著
79 金兹堡-朗道方程 2002.8 郭柏灵等 著
80 排队论基础 2002.10 孙荣恒、李建平 著
81 算子代数上线性映射引论 2002.12 侯晋川、崔建莲 著
82 微分方法中的变分方法 2003.2 陆文端 著
83 周期小波及其应用 2003.3 彭思龙、李登峰、谌秋辉 著
84 集值分析 2003.8 李雷、吴从炘 著
85 数理逻辑引论与归结原理 2003.8 王国俊 著
86 强偏差定理与分析方法 2003.8 刘文 著
87 椭圆与抛物型方程引论 2003.9 伍卓群、尹景学、王春朋 著
88 有限典型群子空间轨道生成的格（第二版） 2003.10 万哲先、霍元极 著
89 调和分析及其在偏微分方程中的应用（第二版） 2004.3 苗长兴 著
90 稳定性和单纯性理论 2004.6 史念东 著
91 发展方程数值计算方法 2004.6 黄明游 编著
92 传染病动力学的数学建模与研究 2004.8 马知恩、周义仓、王稳地、靳 祯 著
93 模李超代数 2004.9 张永正、刘文德 著
94 巴拿赫空间中算子广义逆理论及其应用 2005.1 王玉文 著
95 巴拿赫空间结构和算子理想 2005.3 钟怀杰 著
96 脉冲微分系统引论 2005.3 傅希林、闫宝强、刘衍胜 著

98　生存数据统计分析　2005.12　王启华　著
99　数理逻辑引论与归结原理(第二版)　2006.3　王国俊　著
100　数据包络分析　2006.3　魏权龄　著
101　代数群引论　2006.9　黎景辉　陈志杰　赵春来　著
102　矩阵结合方案　2006.9　王仰贤　霍元极　麻常利　著
103　椭圆曲线公钥密码导引　2006.10　祝跃飞　张亚娟　著
104　椭圆与超椭圆曲线公钥密码的理论与实现　2006.12　王学理　裴定一　著